JOURNAL OF INDIAN ECONOMY AND BUSINESS
Vol. 2, Nos. 1-2, 2025, pp. 1-15 • ISSN: 3048-5789

URL: http://www.pbjournals.com/jieb
Publisher of Open Access Journals

CYBER RISKS IN INDIAN BANKS: A STUDY OF THE COSMOS BANK CYBER ATTACK OF 2018

Amita Dharmadhikary- Yadwadkar[1] and Vikram Aarne[2]
[1]*Assistant Professor, Department of Economics, Savitribai Phule Pune University, Pune, Maharashtra, India*
[2]*Ph. D Scholar, Department of Economics, Savitribai Phule Pune University, Pune, Maharashtra, India.*
Corresponding Author E-mail: amitayadwadkar@gmail.com/amita_dy@unipune.ac.in

Article History
Received : 14 March 2025; Revised : 20 April 2025; Accepted : 26 April 2025; Published : 25 November 2025

Abstract: India's digital financial and banking sector faces a growing challenge of cybercrime and technical glitches. This paper attempts to study and understand the Cosmos Bank cyber attack of 2018. The study uses the analytical approach on secondary data. We found that the attack was a highly sophisticated and well coordinated one. It involved compromising the Core Banking System of the bank by using malware sent through emails and thus enabling several fraudulent transactions on ATMs and through SWIFT to go undetected. The study points out the vulnerabilities in the system and this gives the direction in which the bank and other banks need to work to cover these vulnerabilities.

Keywords: Cyber risks, Indian banks, Cosmos Bank, ATM, SWIFT.

JEL Classification Codes: G00 (General Financial Economics), G20 (Financial Institutions and Services General), G21 ((Financial Institutions and Services Banks)

I. INTRODUCTION

The Indian financial sector is currently undergoing a remarkable transformation. Digital banking, mobile wallets, and online investment platforms have revolutionized accessibility to the financial sector. However, this digital revolution comes with the threat of cybercrime and technical glitches. Financial institutions, holding sensitive data like account details, credit card information, and transaction history are prime targets for

To cite this paper:
Amita Dharmadhikary- Yadwadkar & Vikram Aarne (2025). Cyber Risks in Indian Banks: A Study of the Cosmos Bank Cyber Attack of 2028. *Journal of Indian Economy and Business*. 2(1-2), 1-15.

cybercrimes (Sardana et al., 2024). These cybercrimes can range from stealing financial data through phishing scams to disrupting critical financial services with malware. The consequences can be severe, leading to financial losses, reputational damage, and a loss of consumer trust.

The Cosmos Bank cyber-attack in India in August 2018 is one such case of a cyber-attack which lead to losses of about Rs. 94 crores where hackers used a combination of malware and fraudulent SWIFT (The Society for Worldwide Interbank Financial Telecommunication) transactions to steal the amount.(Jadhav, 2018, Osborne 2018, Kulkarni and Haygunde, 2023, Patel 2023). In another case, a technical malfunction plagued UCO Bank's **IMPS** (Immediate Payment Service System) in November 2023. Over several days, approximately 41,000 UCO Bank accounts received unintended deposits totaling Rs. 820 crores.(IANS, 2023). In 2017, hackers targeted Union Bank of India for a massive heist of nearly Rs. 110 crores. They tricked an employee of the bank with a fake email, disguised as an official message, containing malware. This malware stole money transfer codes. In this case the bank caught the theft before any money was lost. (India Today Webdesk, 2017)

The above incidents are only a few among many such. These highlight the vulnerability of the cyber-banking system to hackers and technical glitches. Recovering stolen funds from cybercriminals is fraught with technical and legal hurdles. Tracing the exact origin of the theft is challenging due to the complex nature of cybercrime. Additionally, understanding the technical intricacies of the crime is often difficult, hindering investigations. Effective response requires coordination among international agencies, which can be hampered by cooperation issues and inefficiencies (Matta et al., 2022). Hence it is essential to understand the vulnerable areas of the working of the cyber financial systems in order to suggest ways to minimize these problems or cyber-attacks. To this end, we intend to study and analyse the Cosmos Bank cyber-attack of August 2018. This will enable us firstly to understand the workings of the system and secondly to identify the vulnerable areas.

We undertook a brief review of literature to see if this has been studied earlier.

II. REVIEW OF LITERATURE

We did not find many detailed studies on the Cosmos bank cyber-attack in literature. We found some studies which reported it and analysed its impact.

There were also studies analyzing similar banking cyber crimes. The literature review is divided into two sections. The first section investigates the factors associated with individual cyber-attacks, drawing upon existing research. The second section focuses on cybercrimes which target the banking and financial sector, analyzing specific incidents and their broader contexts.

2.1. Cyber-attacks on Individuals

Ray (2022) examines digital financial fraud in Jamtara, a district in the Jharkhand state of India which has emerged as a hub for cybercrime involving minors and young adults. Their paper aims to identify the tools and techniques used by cybercriminals and to understand various challenges faced by law enforcement agencies while solving these cyber fraud cases. Their data was gathered through primary sources through interviews and observations of police officers in Jamtara.

According to Ray (2022), these individuals engage in phishing scams, making unsolicited calls to people across the country and deceptively obtaining ATM card details and One-Time Passwords (OTPs) to steal money from bank accounts. Ray's (2022) findings reveal that over half of cybercrimes in the region originate from Jamtara. Ray (2022) finds that most of the frauds uncovered were relatively low-tech in nature. Offenders commonly posed as bank representatives, convincing victims to share confidential details such as Personal Identification Numbers (PINs), account numbers, or one-time passwords, which were then used to divert funds to fraudulent or proxy accounts. Card cloning and phishing were also reported as widespread practices.

Ray's (2022) study pointed out that one of the most serious challenges in tackling these crimes is the issue of jurisdiction. Cyber fraud often crosses state and national boundaries, but policing in India is a state subject, this means rules and procedures vary across states. This lack of uniformity frequently causes delays and hinders the smooth investigation of interstate crimes. Further, Ray (2022) says that many police officers lacked awareness and the technical training necessary to handle cybercrime cases; some continued to register these cases under irrelevant sections causing delays in investigations.

Ray (2022) also finds that the investigation process was slow as a result of weak coordination between police, banks, telecom providers, and

forensic labs. Forensic examination of seized devices often took months, delaying trials and reducing the chances of conviction. The study also noted that conviction rates in cyber fraud cases remain low. This was because of manpower shortages and outdated investigation techniques and also due to limited cooperation from victims, who did not support investigation or court proceedings.

2.2. Cyber-attacks on Financial Institutions

Kedia and Barman's (2023) study examines the current state of cybercrime in India with particular reference to the banking sector. The study was based on quantitative methodology and used secondary data obtained for the time period of 2016–17 to 2020–21.

Kedia and Barman (2023) find a steep increase in cyber financial crimes within the banking system over the past decade with the sharpest jump occurring between 2016–17 and 2017–18, when incidents multiplied almost twenty-five times. In terms of types of fraud, credit and debit card scams, ATM frauds, net banking frauds, and OTP-related crimes were found to be the most prevalent. The financial value of these crimes also increased, especially between 2016–17 and 2017–18. The authors also note that recoveries by banks were minimal compared to the lost amount. Even when the fraud was identified, only a fraction of the stolen money was traced and returned. The paper underscores the vulnerability of the banking sector to cyber threats due to its reliance on digital technologies. (Kedia and barman, 2023)

In the paper by Paul et al (2023), the authors highlight an increase in the number and value of bank frauds and the long time it takes for these frauds to come to light. The authors undertook a survey of 47 respondents (36 bank managers and 11 chartered accountants) who had experience in handling fraud-related issues and belonged to public sector banks such as SBI, Canara Bank, Indian Overseas Bank, and Union Bank of India.

Paul et al (2023) find that the majority of frauds occurred in credit/loan and advances, often due to non-compliance with RBI guidelines, misuse of discretionary powers, and pressure to meet targets. Both auditors and managers agreed that internal audits are valuable but stressed the need for more frequent and specialized audits, including forensic audits. A significant proportion also pointed to employee connivance and political interference

as key enablers of fraud. The study revealed gaps in fraud reporting, nearly 42% of managers admitted that cases often go unreported to RBI or CBI due to reputational risks, recovery concerns, or political pressure (Mohapatra, 2016). They note that conviction rates remain below 26%, with pendency rates for economic offences exceeding 95%, reflecting weak judicial and investigative capacity. To address these, both managers and auditors recommended reforms such as centralized loan processing hubs, stricter verification of collateral, appointment of auditors by the RBI rather than by banks, greater protection for whistleblowers, and the creation of an independent fraud-monitoring body at the state level.

Regarding the detection time Paul et al (2023) find that on an average, smaller frauds take about 24 months to surface, while large-value frauds above ₹100 crore may go undetected for more than five years.

Dhaarani and Ameer (2023) studied the balance sheets of the Cosmos Bank to study the impact of the 2018 cyber-attack on the bank's profits and other parameters. They find that the cyber-attack resulted in significant financial losses, operational disruptions and reputational damage to the bank.

The review of literature undertaken highlights the increasing prevalence of cybercrime in India, particularly financial fraud. Studies by Ray (2022), Paul et al. (2023), Kedia and Barman (2023) and Dhaarani and Ameer (2023) identify various factors contributing to these crimes, including lack of adherence to RBI guidelines, inadequate security measures, and easy access to internet technology. It also reveals that these cybercrimes take a long time to get detected.

3. RESEARCH GAP, OBJECTIVES OF THE STUDY AND METHODOLOGY

3.1. Research Gap

The brief review of literature shows that cyber financial crime targeting both, individuals and institutions like banks, are on the rise resulting in adverse impact on both. Cyber-crimes targeting individuals will have to be dealt with differently; it would involve making individuals more vigilant while using the digital payments systems. However, cyber-crimes affecting institutions are more serious as they impact several individuals at a time and also affect the institution. Institutional cyber-attacks are complex and the solution to

prevent institutional cyber-crimes is therefore not very straightforward. Hence, it is important to study institutional level cyber-attacks to understand how they are undertaken and how they can be prevented. Given this, we aim to study one case of institutional cyber-attack; namely the Cosmos bank cyber-attack of 2018.

3.2. Objectives of the Study

- To understand how the cyber-attack on Cosmos Bank of 2018 occurred.
- To ascertain the reasons and the vulnerabilities of the system which led to the cyber-attack on Cosmos Bank in 2018

3.3. Methodology

In this study we have used the analytical approach. We have used secondary data sources, namely reports, articles and news reports through videos etc. to understand how the cyber-attack on Cosmos Bank took place. This attack, analyzed extensively by Securonix, a leading cyber security firm, provides insights into attack modalities, detection strategies, and the challenges faced by financial institutions and payment networks like VISA[1] and NPCI[2] (National Payments Corporation of India). The paper is presented in three sections: Section IV discusses the Cosmos bank cyber attack of 2018; Section V discusses the red flags or warning signals which had emerged and Section VI presents the conclusions and suggestions.

4. THE COSMOS BANK CYBER ATTACK OF 2018

In August 2018, the Cosmos Cooperative Bank (CCB) one of India's oldest cooperative banks, based in Pune, became the victim of a highly sophisticated cyber-attack. This was a two pronged cyber-attack in which the attacker siphoned off approximately Rs 94 crores through a combination of ATM fraud and SWIFT system exploitation. On August 11th 2018, the Cosmos Co-operative Bank suffered a major cyber-attack targeting its ATM infrastructure. This attack was followed by another on August 13th, 2018, which compromised the SWIFT infrastructure.

4.1. The Cosmos Cooperative Bank

Established in 1906 in Pune, Maharashtra, Cosmos Co-operative Bank is a key player in India's banking sector with a century-long legacy of robust

financial performance. In 2023-24, the bank reported a net profit of ₹384 crore. Serving over 1.2 million customers, including individuals, businesses, and organizations, it operates 183 branches across seven states: Maharashtra, Gujarat, Madhya Pradesh, Karnataka, Andhra Pradesh, Telangana, and Tamil Nadu. Headquartered in Pune with around 1,500 employees, the bank prioritizes customer satisfaction and financial stability, contributing to India's economic growth. While Cosmos Bank has no physical international branches, it supports global customers through foreign exchange services, Non Resident India (NRI) or Person of Indian Origin (PIO) accounts, and correspondent relationships with over 110 banks worldwide.

Cosmos Bank's online transaction system features CosmoNet, a secure and user-friendly internet banking platform for most retail services. Its mobile app supports account balance checks, fund transfers, bill payments, and deposits. The bank facilitates transactions via National Electronic Funds Transfer (NEFT), Real Time Gross Settlement (RTGS), IMPS, and United Payments Interface (UPI), with set daily limits. Its ATM network, comprising 142 ATMs and five cash recycling units, enables balance inquiries, cash withdrawals, and basic transactions. Although specific international ATM numbers are unavailable, Cosmos Bank's RuPay and Visa debit cards are likely accepted at global ATM networks.

4.2. The Sequence of Events

On Friday 11 August 2018, the Cosmos Cooperative Bank in Pune received an urgent call from Visa. The card network had detected an abnormal pattern in the bank's systems- an unusual surge of transactions had occurred within the span of just one hour. As a result, Visa alerted Cosmos Bank, urging them to investigate immediately. Responding to this, Cosmos Bank's staff began checking their internal systems. Strangely, nothing seemed problematic. The bank's servers showed no sign of compromise, no internal alerts of fraud. The matter seemed contained at that time. But in reality, the bank was already under siege.

4.3. The ATM Card Network Attack (VISA and Ru-Pay)

The ATM attack was a highly coordinated operation in which "money mules" were stationed in 28 countries including Canada, Hong Kong, the United Kingdom, the United Arab Emirates, Turkey, Japan, Russia, and

the United States. Within two hours and thirteen minutes, nearly 12,000 transactions were fraudulently processed through ATMs using VISA debit cards, amounting to ₹81.99 crore. The money mules operated with strict discipline. They were instructed to wear caps, cover their faces, and move quickly between ATMs to avoid detection.

Within India, 2,800 fraudulent transactions worth ₹2.75 crore were executed from domestic ATMs using Rupay cards within a span of just four hours. The most significant concentration of withdrawals occurred in Kolhapur, Maharashtra, where ATM surveillance footage revealed small groups of individuals conducting repeated transactions at multiple ATMs. Apart from Kolhapur, similar withdrawals were reported in Pune, Mumbai, Jaipur, and Indore, indicating a widespread and synchronized effort.

The roots of the siege can be traced back to months before the attack happened. Hackers sent highly targeted spear fishing emails to bank employees. These emails carried carefully crafted attachments which, once opened, released malware into the bank's system. This gave the attackers a foothold and allowed them to gradually expand their access deeper into Cosmos Bank's network. This also provided the hackers access to the ATM Switch.

On the day of the heist, the hackers infiltrated payment system connected to Cosmos Bank. Within just few minutes, thousands of fraudulent withdrawal requests were generated. Although Visa's system initially flagged these as suspicious, the attackers had already disabled Cosmos Bank's internal servers that should have synchronized and validated the data. This meant the fraudulent transactions could not be cross-checked in real time.

4.3.1. How the ATM Switch Works

The ATM switch is the central system that connects a bank's ATMs with external payment networks such as Visa or Mastercard. When a customer inserts their card and enters a PIN, the request is first routed through the bank's ATM switch. The switch then communicates with the bank's core banking system to verify the card details, confirm the PIN, and check whether sufficient funds are available in the account. In the case of international or non-home bank cards, the switch sends the request to global payment gateways (for example, Visa). The gateway then approaches the respective bank for approval. Once the bank verifies and confirms, the approval

message travels back through the same chain from Visa to the ATM switch and the ATM allowing the cash withdrawal to take place.

The Core Banking System (CBS) receives debit card payment requests via its 'Switching System'. But during the malware attack, a proxy switch was created and all the fraudulent payment approvals were passed through this proxy switching system. As a result, withdrawals were carried out seamlessly across multiple countries.

4.3.2. How the Hackers Cloned the Cards

The attackers behind the Cosmos Bank heist used the ATMs to withdraw cash by cloning debit cards. They obtained legitimate customer card data by breaching Cosmos Bank's internal servers and extracting sensitive information such as card numbers, expiry dates, and magnetic stripe details**.** Then this data was transferred onto blank magnetic stripe cards using specialized encoding devices. These counterfeit cards behaved exactly like real debit cards when inserted into an ATM.

To make the cloned cards work, the hackers disabled parts of Cosmos Bank's systems that would normally validate transactions against actual balances. As a result, when these counterfeit cards were used, the ATMs accepted them as genuine, even though no real funds were linked to those cards. (BBC 2023 a, 2023, b)

4.3.3. How the Hackers Found the PIN

PIN (Personal Identification Number) is essential for ATM withdrawals. The hackers managed to obtain PINs because they had infiltrated Cosmos Bank's internal networks. Through this access, they could intercept or directly extract encrypted PIN verification data stored within the bank's systems. The hackers had the PIN stolen from the compromised servers. (BBC News 2023 a, 2023, b)

4.3.4. Investigation of the ATM Attack

To identify the perpetrators, law enforcement authorities analysed mobile phone data, correlating device activity with the timing and locations of the suspicious withdrawals. This analysis supported the identification of individuals involved in the coordinated operation. (BBC 2023 a, 2023, b). In 2023, 11 people were arrested for this. (Press Trust of India, 2023)

4.4. The SWIFT System Compromise

The Cosmos bank cyber-attack also comprised of a fraudulent transfer of ₹13.92 crore to the account of M/s. ALM Trading Limited at Hang Seng Bank in Hong Kong via the SWIFT payment gateway. (Kolesnikov and Securonix Threat Research Team, 2021)

The Society for Worldwide Interbank Financial Telecommunications, or SWIFT, is a large-scale messaging network that serves as the foundation for the majority of international money and security transfers. It functions as a secure and efficient communication system, allowing financial institutions to exchange information, including instructions for money transfers. SWIFT enables individuals and businesses to process electronic and card payments even when the payer and payee use different banks. The network operates by assigning each member institution a unique 11-digit BIC (Bank Identifier Code) that specifies the bank, country, city, and branch.

For instance, if a customer at a Bank of America branch wishes to send money to a friend in Venice, Italy, who banks with UniCredit Banca, they would provide their friend's account details and the specific UniCredit Banca branch information, including its unique SWIFT code. Bank of America would then transmit a payment transfer message to the UniCredit Banca branch through the secure SWIFT network. Upon receiving this message, UniCredit Banca would process the payment and deposit the funds into the friend's account. (Seth, 2023)

On Monday August 13, 2018, two days after the ATM fraud, hackers targeted Cosmos Bank's SWIFT infrastructure. They exploited compromised credentials and bypassed authentication mechanisms to initiate unauthorized fund transfers. The funds were directed to an account in Hong Kong, specifically to ALM Trading Limited at Hang Seng Bank, amounting to approximately ₹13.92 crores. (Press Trust of India, 2023; Risk Quotient, n.d.)

5. THE RED FLAGS OR WARNING SIGNALS IN THE SYSTEM

Several red flags or warning signs emerged in the system during the attack. In the study by Kolesnikov and the Securonix Threat Research Team (2021), the authors point out several warning signals which occurred in the system but were either not recognized by the bank officials or were cleverly disabled by the cyber criminals so that they could not alert the bank officials. According to Kolesnikov and STRT (2021) the following should have been red flags:

(a) **Unusual ATM Activity:** A sudden surge in ATM transactions, particularly those originating from unusual locations, raised red flags. For instance, the high volume of transactions in a short period was a significant anomaly.

(b) **Abnormal Network Traffic:** Unusual patterns, such as unexpected connections to certain external IP addresses indicated malicious activity.

(c) **Unauthorized Access to Critical Systems:** Detection of unauthorized access to sensitive systems, including the ATM switch and SWIFT environment, was crucial. This involved monitoring for rare processes and modifications, such as changes to the check Pan() transport layer function and Generate Response Transaction{1,2}() functions, suggesting deep system manipulation

(d) **Malicious Code Execution:** The execution of malicious code, including malware with specific hashes was identified. Attack techniques included Windows Admin Shares for lateral movement, adding new services for persistence, Windows Firewall changes, Time stomping, and Reflective DLL Injection, all indicative of a sophisticated attack. (Kolesnikov and STRT, 2021)

5.1. The Role of Malware and System Manipulation

According Purukayastha (2018) a critical aspect of the attack was the malware's impact on the bank's switching system. The malware created a proxy switch system, bypassing the core banking system (CBS) and approving fraudulent payment requests without proper validation. This manipulation meant that ATM transactions, while processed, were not subjected to normal security checks, potentially preventing them from being flagged as abnormal by the bank's internal monitoring. Thus it is likely that the legitimate switching system's inability to process or flag these transactions was due to the proxy's interference.

5.2. Why Couldn't Cosmos Bank Foil the Attack?

Although VISA alerted the Cosmos bank on 11th August towards an abnormally heightened withdrawal activity, the bank officials could not find any problem in their system. This was obviously due to the fact that the

malware had compromised the CBS of the bank. According to Purukayastha (2018) Indian banks have only moderate security and smaller banks with less sophisticated security could be more prone to such cyber attacks. He further writes that prior to this attack the American FBI (Federal Bureau of Investigation) had issued a warning of a large scale world-wide threat of a malware attack on ATMs.

It is no doubt that the Cosmos bank cyber attack was a very sophisticated one involving a world- wide coordination. In the face of such sophisticated attack the Cosmos bank system could not stand ground. This whole incident points to a need to revamp security of cyber and digital payment systems in banks. Smaller banks are more vulnerable and hence need to take appropriate precautions. It is also to be noted that such cyber attacks are carried out on Saturdays so that they do not get detected soon.

6. FINDINGS, CONCLUSIONS AND SUGGESTIONS

India's digital financial sector faces a growing challenge of cybercrime. This paper attempted to study and understand the Cosmos Bank cyber attack of 2018. We found that the attack was a highly sophisticated and well coordinated one. It involved compromising the Core Banking System of the bank by using malware sent through emails and thus enabling several fraudulent transactions on ATMs and through SWIFT to go undetected. The study points out the vulnerabilities in the system and this gives the direction in which the bank and other banks need to work to cover these vulnerabilities.

Banks, especially smaller banks need to enhance their cyber security procedures. The following recommendations can be made in this regard.

1. Firstly the staff should be trained to detect warning signals in the cyber system and to respond to these.
2. Secondly, during routine training, possible scams should be visualised and awareness should be created about this among the employees.
3. Thirdly there should be regular system audits like fire audits to test whether the system is able to resist the scam or gives in to the scam.
4. Fourthly it has been noticed that these scams or attacks generally take place mostly on Fridays or Saturdays, just before the weekend is to begin. Extra vigilance should be exercised during this time.

The Cosmos Bank cyber attack should be taken like a lesson for the banking system to upgrade and enhance security measures. As more and more of Indians embrace the digital system it becomes even more imperative to enhance the cyber security measures to ensure a robust, glitch free and scam free digital banking and payment systems.

Notes

1. VISA is a global payment technology company that provides electronic payment services worldwide.
2. NPCI (National Payment Corporation of India) is an organization that manages India's digital payment systems including RuPay, UPI and others.

References

Acharya Suman and Joshi Sujata.2020. "Impact Of Cyber-Attacks On Banking Institutions In India: A Study Of Safety Mechanisms and Preventive Measures" ; *Palarch's Journal of Archaeology of Egyp*t/Egyptology 17(6) ISSN 1567-214x https://archives.palarch.nl/index.php/jae/article/view/1714/1708

BBC News. 2023 a. The Lazarus Heist: Cosmos Bank Robbery [Video]. August 29th YouTube. https://www.youtube.com/watch?v=2npt0bK9oj4&t=23s

BBC News. 2023. b. *The Hacker Hiding in the Dark Web – The Lazarus Heist, Season 2 Episode 2* ,March 14). [Video]. YouTube. https://www.youtube.com/watch?v=VXv9-GftmmM

Cosmos Bank 113th Annual Report 2018-19 https://www.cosmosbank.com/auth/writereaddata/files/110521193370101_Cosmos-Bank-AR-2018-19_web.pdf

Dhaarani S. and Aaliya Ameer. 2023. "A Case Study on Cyber Security Threats to Cosmos Bank"; *Indian Journal of Integrated Research in Law Volume* III Issue VI | ISSN: 2583-0538 November 2023 to December 2023. Page:505-518 https://ijirl.com/volume-iii-issue-vi/

IANS .2023. 2023. "UCO Bank Stops Online Transfers After a Series of Flawed Payments, in Economic Times (November 16, 2023) https://government.economictimes.indiatimes.com/news/secure-india/uco-bank-stops-online-imps-transfers-after-a-series-of-flawed-payments/105262092

India Today Webdesk .2017. "When Cyber Criminals Nearly Looted USD 170 Million from Union Bank of India" India Today, April 12, 2017 https://www.indiatoday.in/india/story/cyber-theft-union-bank-of-india-theft-hackers-170-million-dollars-970855-2017-04-11

Jadhav Rajendra 2018. Cosmos Bank Loses $13.5 Million in Cyber-attack, Reuters, (August 14, 2018); https://www.reuters.com/article/world/cosmos-bank-loses-135-million-in-cyber-attack-idUSKBN1KZ1J8/

Kedia Radhika and Barman Prateeksha. 2023. "Cyber Crime in India With Reference to Banking Sector"*; Rabindra Bharati Journal of Philosophy* ISSN: 0973-0087Vol.: XXV, No. : 04, 2023

Kulkarni Sushant and Haygunde Chandan .2024. Pune Crime Files: Cyber-attack on Cosmos Bank That Funneled Rs 94 Crore in Just 3 Days, in The Indian Express, 19th Feb 2024. https://indianexpress.com/article/cities/pune/pune-crime-files-cyber-attack-cosmos-bank-funnelled-rs-94-crore-9168771/

Kolesnikov Oleg and Securonix Threat Research Team. 2021. Cosmos Bank SWIFT/ ATM US$ 13.5 Million Cyber Attack Detection Using Security Analytics, Report https://www.securonix.com/wp-content/uploads/2021/07/Securonix_Cosmos-Bank-Report.pdf

Matta, R., Kochhar, K., Mohapatra, A. K., & Mohanty, D. (2022). Board Characteristics and Risk Disclosure Quality by Integrated Reporters : Evidence from Indian Banks. *Prabandhan: Indian Journal of Management*, *15*(5), 27–42. https://doi.org/10.17010/pijom/2022/v15i5/169579

Mohapatra, A. K. (2016). Role of MUDRA Bank in Financing Non-Corporate Small Business Sectors. *Review of management*, *6*.

Osborne Charlie. 2018. How Hackers Managed to Steal $13.5 Million in Cosmos Bank Heist in ZDNET/tech 27th August, 2018. https://www.zdnet.com/article/how-hackers-managed-to-steal-13-5-million-in-cosmos-bank-heist/

Patel Dharam .2023. Case Study; 2018 Pune's Cosmos Bank Cyber-Attack in Medium.com, 31st March 2023. https://medium.com/@20dcs071/case-study-2018-punes-cosmos-bank-cyber-attack-cafd221cac25

Paul Sanu, Haridas Manju and Prasad K D V.2023. "Bank Frauds: An Empirical Analysis on Need for Robust Legal Mechanism"; *Lex Humana*, v.15,n.2, 2023,ISSN 2175-0947 Universida de CAtolica de Petropolis, Rio de Janerio, Brasil

Press Trust of India. 2023. 11 Convicted in India's Biggest Cyber-attack on Cosmos Bank. NDTV. 24th April, 2023. https://www.ndtv.com/india-news/11-convicted-in-indias-biggest-cyberattack-on-cosmos-bank-3973428

Purukayastha Rajarshi. 2018. Lessons Learnt From Cosmos Bank Attack; Tata Communication Blog., 18th September, 2018. https://www.tatacommunications.com/blog/2018/09/lessons-learnt-from-cosmos-bank-attack/

Ray Pranav Kumar. 2022. "A Study on Cyber Financial Frauds in The District of Jamtara, Jharkhand"; *Journal of Forensic Science and Research* ISSN 2575-0186 https://doi.org/10.29328/journal.jfsr.1001034

Risk Quotient (n.d.) Bank Cyber Heist Analysis. https://www.rqsolutions.com/bank-cyber-heist-analysis.html

Sardana, V., Mohapatra, A. K., Singhania, S., & Chakrabarti, D. (2024). Changing Dynamics of Banking Landscape : What Do We Know and What Lies Ahead?. *Prabandhan: Indian Journal of Management*, *17*(1), 8–23. https://doi.org/10.17010/pijom/2024/v17i1/173288

Seth,S.2023. What is the SWIFT banking system? in Investopedia. September 14,https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp