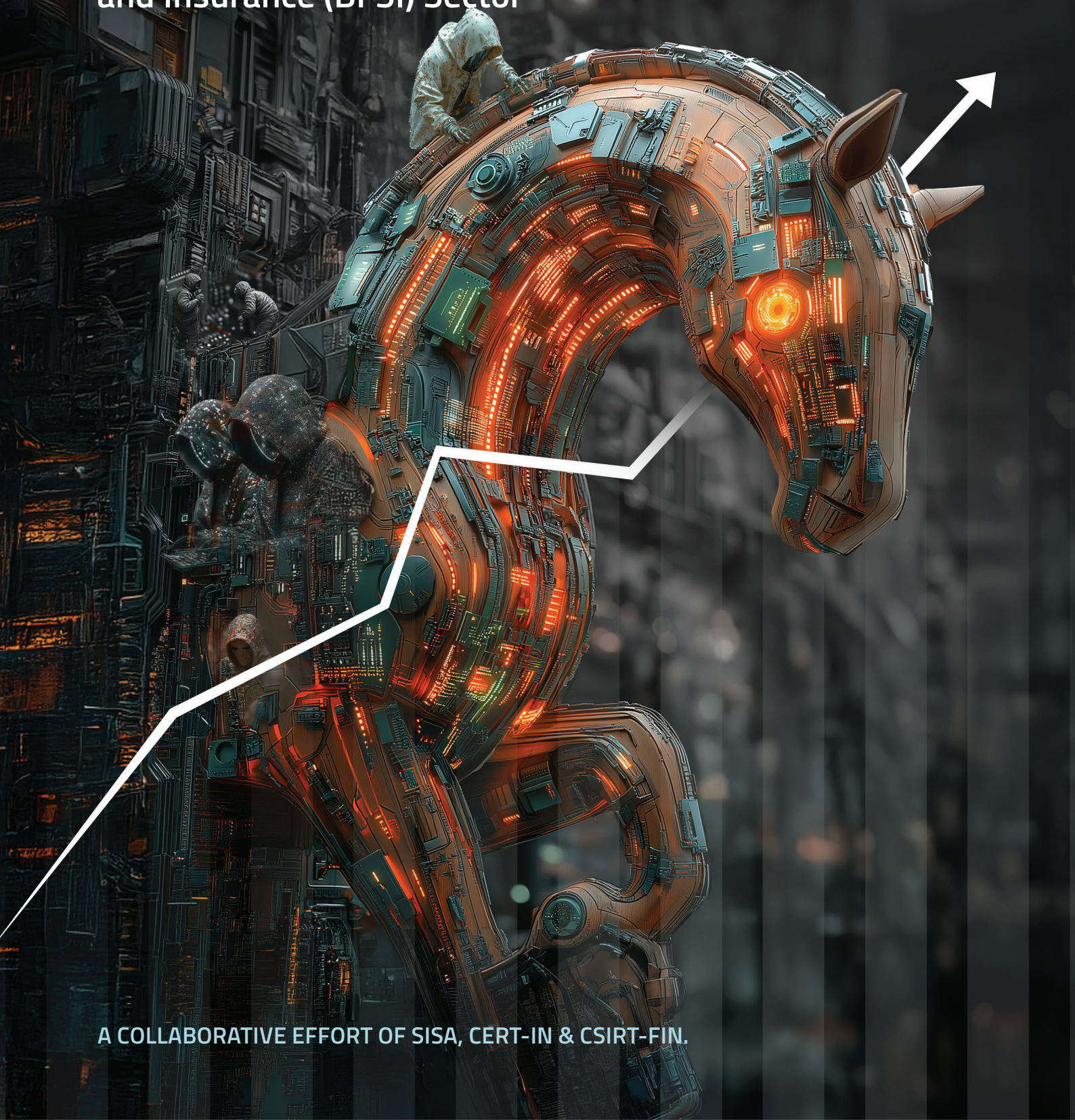
SISA

certin
Enhancing Cyber Security in India

CSIRT-Fin

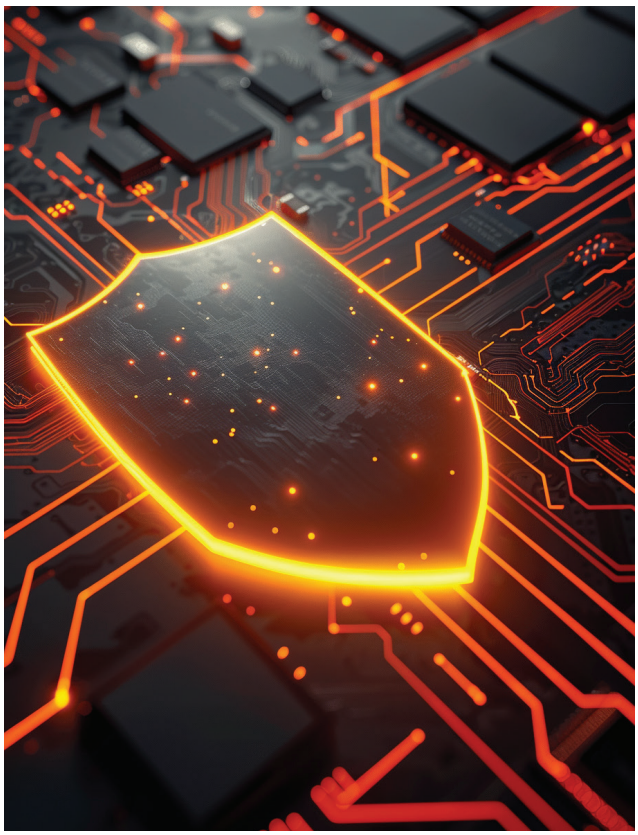
DIGITAL THREAT REPORT 2024

For the Banking Financial Services and Insurance (BFSI) Sector



A COLLABORATIVE EFFORT OF SISA, CERT-IN & CSIRT-FIN.

CONTENTS



PREFACE

Finance sector not just in India but across the globe is undergoing rapid digital transformation and adopting new technology-driven solutions. Though, technology intervention helps streamline processes and customer service delivery, it also expands the security threat landscape, necessitating need for a robust and effective cyber security framework.

As the sector continues to adopt Fintech and digital solutions, cyberattacks are growing more sophisticated, frequent, and targeted. A cyberattack on a financial institution can have disastrous results. Cyberattacks in financial institutions can have systemic effects that are exacerbated by technological and financial ties between other financial and non-financial institutions, resulting in exponential losses.

Thus, efficient, and effective response to and rapid recovery from a cyber incident by financial organisations are essential to limit these financial stability risks. Further, considering the interconnectedness and interdependency of financial entities and the borderless nature of cyber incidents, the cyber risk of any given entity is no longer limited to the entity's owned or controlled systems, networks, and assets. Further entities which were not the primary target or source of disruption may also be affected. Hence, it becomes much more important for authorities to coordinate at sector/national level.

CERT-In and CSIRT-Fin are playing a critical role by coordinating with various global & national financial organisations, regulators, national CERTs and other government agencies in rendering a timely and efficient cyber incident response to contain, reduce, or even eliminate cyber risk.

CERT-In and CSIRT-Fin have noticed a clear pattern in which cyberattacks in the financial industry are becoming more complicated and sophisticated. Malicious actors use sophisticated tactics, techniques and procedures to plan these attacks in order to get beyond traditional defenses. The cyber security landscape is changing in tandem with the spread of cutting-edge technologies like cloud computing, Application Programming Interfaces (APIs), and Artificial Intelligence/Machine Learning (AI/ML). Notable findings also show that some firms still struggle with basic cyber hygiene procedures and do not follow established security policies and procedures.

The report prepared by CERT-In, CSIRT-Fin and SISA offers an in-depth analysis of the evolving cyber threat landscape, focusing on the methods, tactics, techniques and procedures (TTPs) employed by threat actors targeting the BFSI sector. It provides a comprehensive overview of the methods malicious actors use to exploit vulnerabilities in BFSI organizations. The report outlines practical, actionable recommendations that organizations in the BFSI sector can implement across three pillars of the people, process, and technology. These include key security controls and mitigation strategies designed to fortify defenses and reduce vulnerabilities.

The report's timely insights will help organizations to better safeguard their assets by taking proactive steps in enhancing their security postures and preparing for potential future breaches before they occur. The report also promotes sector-wide collaboration, allowing organizations to learn from each other's experiences and improve resilience of individual organizations as well as strengthen the BFSI sector as a whole by facilitating team work through a collective response to emerging cyber threats.

S. KRISHNAN, I.A.S.
Secretary,
Ministry of Electronics & Information Technology, (MeitY),
Government of India

INTRODUCTION

Welcome to the 2024 Digital Threat Report for the BFSI Sector. This report represents a convergence of insights from cybersecurity leaders, bringing together the strengths of frontline solution providers, national agencies, and expert responders. By pooling real-world data, early threat detection capabilities, and incident handling expertise, we have created a comprehensive view of the most critical risks facing the industry today. The collaborative nature of this report ensures that organizations gain visibility from multiple vantage points—providing a holistic understanding of adversary tactics, techniques, and procedures.

In an era where cyber threats evolve at an unprecedented pace, resilience is no longer optional—it is the foundation of organizational strength. This resilience emerges when compliance and security are viewed not as separate endeavors but as interconnected pillars of a unified strategy. When harmonized, they empower organizations to anticipate vulnerabilities, respond proactively, and build a formidable defense against emerging threats.

The 2024 Digital Threat Report for the BFSI Sector reflects this principle, combining intelligence from root cause analysis of cyber incidents conducted by CSIRT-Fin team, and forensic investigations conducted by SISA. It serves as a vital resource for navigating a landscape where security and compliance are not just essential but mutually reinforcing. It underscores the growing interdependence between regulatory frameworks and security practices. The insights offered are not merely reactive; they are forward-looking, designed to help organizations anticipate challenges and drive sustained readiness for the future.

The BFSI and digital payments industries lie at the heart of global digital transformation. Projected to generate $3.1 trillion by 2028—accounting for 35% of total banking revenue—this sector's transition from cash to digital transactions introduces immense opportunities alongside heightened risks. As digital payments grow, they increasingly attract malicious actors who exploit system vulnerabilities, making this sector a prime focus for cyberattacks.

From threats targeting cloud identities and infrastructure to sophisticated attack patterns on digital applications, the report explores how adversaries adapt to evolving technological landscapes. It not only details these emerging threats but also offers practical strategies for emulating and mitigating these risks—empowering businesses to enhance detection and response capabilities.

Our mission is to bridge the gap between awareness and action, equipping organizations to refine their approach to threat detection, response, and long-term resilience. This report delivers intelligence designed to help security teams stay one step ahead, ensuring they are prepared not just for today's challenges but for those that lie ahead.

Together, let's transform challenges into opportunities, safeguarding the digital payments ecosystem to ensure it remains secure, resilient, and ready for the future.

DHARSHAN SHANTHAMURTHY
Founder & CEO, SISA

POINT OF VIEW

Technology has been a driving force in shaping the securities market, enabling greater efficiency, accessibility, and affordability. However, with swift technological advancements, protection of IT infrastructure and data has become a key concern for the securities market regulator Securities and Exchange Board of India (SEBI) and its Regulated Entities (REs). In order to strengthen the cybersecurity measures and to ensure adequate cyber resiliency against cybersecurity incidents/ attacks in Indian securities market, SEBI has issued Cybersecurity and Cyber Resilience.

Framework (CSCRF). CSCRF is a standards based framework and broadly covers the five cyber resiliency goals, viz. Anticipate Withstand, Contain, Recover, and Evolve, which are adopted from CERT-In Cyber Crisis Management Plan (CCMP), for countering Cyber Attacks and Cyber Terrorism.

The Digital Threat Report 2024, developed by SISA in collaboration with CERT-In and CSIRT-Fin, provides critical insights into the evolving attack methods, reinforcing the urgency for market participants to adopt robust security measures, strengthen compliance protocols, and enhance threat detection capabilities.

In my opinion, the research findings mentioned in the report will augment the CSCRF framework towards the implementation of various solutions for cybersecurity and cyber resiliency, thus promoting digital trust, innovation, and sustainable growth.

AVNEESH PANDEY
Chief General Manager and CISO
Securities and Exchange Board of India (SEBI)

The digital payments landscape is evolving at an unprecedented pace. While these advancements improve accessibility and the efficiency of various payment platforms, they also require continuous vigilance.

As a key enabler of India's digital payments infrastructure, the National Payments Corporation of India (NPCI) understands that cybersecurity and resilience are crucial to maintaining public trust and financial stability.

The key threats identified in the Global Threat Report 2024 for the BFSI Sector highlight the growing risks to payment networks, such as real-time fraud, API security gaps, and targeted attacks on financial infrastructures. With the increasing reliance on AI-driven transactions and embedded finance models, safeguarding the payments ecosystem from phishing, malware, and supply chain vulnerabilities is more critical than ever. Recent cyber incidents reinforce the need for multi-layered security strategies, real-time threat intelligence, and AI-enabled technologies to mitigate risks.

This report, developed by SISA in collaboration with CERT-In and CSIRT-Fin, offers insights into the evolving threat landscape, stressing the urgency for payment networks, banks, and fintech players to adopt zero-trust architectures, strengthen compliance frameworks, and enhance cyber resilience and fraud detection capabilities.

I commend the collaborative effort behind this report and encourage all stakeholders across the digital payments industry to use these insights to strengthen security measures, build cyber resilience, and maintain consumer trust in our fast-growing digital economy.

DILIP ASBE
Managing Director and CEO of the National Payments Corporation of India (NPCI)

POINT OF VIEW

The Indian BFSI domain has witnessed rapid digital innovation. it is evolving into a tech-driven ecosystem where digital platforms, advanced analytics, and alternative distribution channels are shaping products and services. While technology is transforming the insurance sector at breakneck speed, regulators and industry players face several interlinked challenges.

Digitization has exposed entities in BFSI sector to cyberattacks, which can compromise sensitive personally identifiable information and disrupt core services.

The use of artificial intelligence to improve efficiency & reduce costs, the proliferation of APIs for delivering personalized services has brought heightened risks to information assets, making cybersecurity a critical focus area for organizations striving to protect their assets, reputation, and customers.

The report highlights some of the major attacks the BFSI sector is facing in the form of Data Exfiltration, Ransomware attacks exposing sensitive client data, Insecure API exploitation leading to unauthorized access, threat of Quantum Computing, third-party data breaches compromising personal information, Internal Threats etc. along with the recommendation for protecting and strengthening the cyber Security posture and resilience of organisations.

The report also highlights the growing interconnectedness of financial systems amplifying the impact of such breaches. Thereby, requiring effective and efficient responses to these incidents, along with rapid recovery mechanisms to mitigate damage and maintain trust.

By collaborating with global and national financial organizations and Regulators, CERT- In and CSIRT-Fin have been providing critical incident response coordination, threat intelligence sharing, and guidance on mitigating cyber risks to BFSI sector. Their efforts are enabling organizations to anticipate and address emerging threats more effectively, thereby improving the resilience of the BFSI sector.

As a Regulator for Insurance Industry, IRDAI has taken various measures to ensure its Regulated Entities have put in place effective controls to protect their information assets in the face of evolving cyber security landscape. The measures include comprehensive guidelines on information and cybersecurity mandating establishment of robust cybersecurity frameworks including technical controls, annual comprehensive audit, incident response policy & plan including forensic, training and awareness and collaboration with industry and Cert-In. These measures aim to strengthen the cybersecurity posture of the insurance industry, ensuring resilience against evolving cyber threats while safeguarding sensitive customer data and maintaining trust.

As the financial sector continues its journey of rapid digital transformation, the importance of robust cybersecurity practices cannot be overstated. By leveraging the expertise of CERTs, implementing actionable recommendations across people, processes, and technology, and taking proactive steps to enhance security postures, organizations can effectively address the evolving cyber threat landscape. The commitment to continuous improvement and vigilance ensures that financial organizations remain resilient in the face of emerging challenges, safeguarding both their operations and their customers.

The report will certainly help the entities in BFSI sector to review their cyber security posture and ensure that their IT systems are resilient to the cyber vulnerabilities.

A.R.NITHIYANANTHAM
Executive Director, IRDAI


HIGHLIGHTS

This report draws on the collective expertise and insights of industry leaders to provide a unified view of the cybersecurity landscape in 2024. It reflects a seamless exchange of knowledge, shaped by real-world cyber incidents, evolving adversarial tactics, and emerging threat intelligence.

By integrating a national perspective on cyber trends with frontline experience in mitigating sophisticated attacks, this report delivers a holistic understanding of the shifting threat environment. The result is a comprehensive resource that empowers organizations to anticipate risks, strengthen defenses, and navigate the complexities of today's cybersecurity challenges.

Over the past year, cyberattacks have grown more sophisticated, driven by the intersection of new techniques and the persistence of proven methods. Social engineering, in particular, has surged to the forefront, with Business Email Compromise (BEC) and advanced phishing campaigns operating with alarming precision. These attacks, often bolstered by data sourced from the dark web, bypass traditional defenses by leveraging stolen credentials and session cookies, effectively neutralizing multi-factor authentication. Meanwhile, supply chain breaches have escalated, exploiting the trust organizations place in third-party vendors and open-source repositories thereby introducing vulnerabilities at scale.

Yet, the rising tide of cyber threats is not occurring in isolation. As digital ecosystems expand, so too does the recognition that compliance must evolve beyond rigid frameworks. This report explores how regulatory landscapes are shifting towards harmonization, with the goal of unifying disparate standards across regions. Compliance is transforming from a burdensome obligation into a strategic enabler—one that can unlock growth, improve operational efficiency, and reinforce resilience in sectors like digital payments, where sensitive data remains a prime target for attackers.

Beneath these strategic shifts lies a more pressing reality—critical control gaps continue to persist across industries. Weak access controls, over-privileged user accounts, and misconfigurations leave even the most fortified organizations exposed. This report highlights how these vulnerabilities are not merely by-products of oversight but structural weaknesses that adversaries consistently exploit to devastating effect.

As the industry braces for what lies ahead, the future of cybersecurity is already being reshaped by artificial intelligence (AI). The same technology that drives innovation is arming attackers with the tools to conduct highly personalized, evasive, and large-scale attacks. In 2025 and beyond, AI-driven threats will challenge existing defense mechanisms, forcing organizations to rethink their approach to threat detection and response.

This report offers concrete recommendations rooted in frontline audits and incident analysis, outlining the steps necessary to close control gaps, strengthen defenses, and build adaptive strategies against emerging threats. The findings presented here serve as both a reflection of the current landscape and a guidepost for navigating the uncertainties of tomorrow.

SPECIFICALLY, THE REPORT AIMS TO:

Illuminate Adversaries' Playbooks

Offer insights into the methods, tactics, and procedures (TTPs) employed by threat actors, including how they exploit vulnerabilities, use AI to enhance their attacks, and target organizations through novel means.

Anticipate Future Attacks:

Predict potential future breaches based on current trends, dark web chatter, and the evolution of attack techniques, enabling organizations to proactively prepare for emerging threats.

Assess the Impact of AI in Breaches:

Explore how AI and machine learning are being utilized by attackers to develop sophisticated malware, automate attacks, create convincing deepfakes, and lower the barriers for cybercriminal activities.

Recommend Preventive and Detective Controls:

Provide actionable recommendations and key controls that organizations can implement across the pillars of people, process, and technology. These preventive and detective measures are designed to fortify defenses, mitigate risks, and enhance overall cybersecurity resilience against both current and emerging threats.

Highlight Current Trends and Select Cases:

Examine recent breaches, including those affecting organizations with robust security postures, to understand how and why these incidents occurred despite strong defenses.

METHODOLOGY & SOURCES

The report is based on a synthesis of various sources, including:

Direct Observations from SISA's DFIR Investigations:

Drawing on select cases and insights gained from digital forensics and incident response (DFIR) projects handled by SISA over the past year.

Cybersecurity Reports and Data Pointers:

Incorporating findings from vulnerability databases, and observed trends in malware and exploit usage.

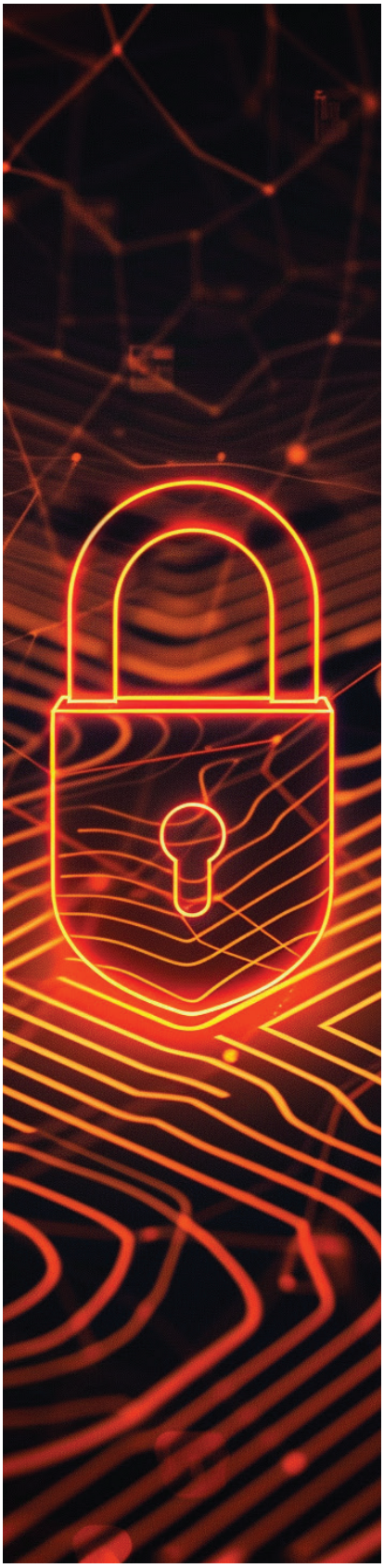
Observations of CSIRT-Fin, CERT-In:

Based on a comprehensive analysis of cyber incidents affecting the BFSI sector, with actionable recommendations for enhancing cyber maturity, data rotection, backup strategies, and recovery measures.

Research and Analysis:

Leveraging research on AI's impact on cybersecurity, including adversarial machine learning, deepfake technology, and malicious use of large language models.

THREAT LANDSCAPE OVERVIEW



Cyber threats are no longer a distant concern—they are an immediate and inescapable reality, particularly for the BFSI industry. In 2024, the sector witnessed a surge in the sophistication, scale, and diversity of cyberattacks, highlighting a rapidly evolving threat landscape. With the average cost of a data breach reaching an all-time high of $4.88 million globally[1]—a 10% increase from 2023—and $2.18 million in India[2] , the financial stakes have never been higher.

The BFSI sector ecosystem faces unique challenges due to its interconnected infrastructure and the high-value financial data it safeguards. This convergence of high rewards and expanding technological complexity has made the sector a prime target for attacks by cyber malicious actors. Phishing and compromised credentials are some of the key forms of cyber-attacks in India.

For the financial sector in India, H12024 alone saw a 175%[3] surge in phishing attacks compared to the same period last year, underscoring the heightened activity within an increasingly volatile threat landscape. Cloud exploits emerged as a critical entry point, exposing gaps in complex infrastructures and amplifying the financial and operational impacts of breaches. Meanwhile, supply chain attacks have evolved to exploit interconnectivity, breaching even the most fortified systems with persistent and adaptive tactics.

As attackers increasingly leverage artificial intelligence (AI), identity-based attacks have grown more sophisticated and pervasive. AI's ability to exploit identity vulnerabilities and bypass defenses using social engineering techniques signals a troubling evolution in cyber tactics. Deepfake technology, for instance, is enabling large-scale impersonation scams, including executive-level Business Email Compromise (BEC) attacks and misinformation campaigns. With India experiencing a higher than average rise in deepfake identity fraud[8], organizations face unprecedented challenges in preserving digital trust.

The average time from vulnerability disclosure to exploitation has decreased dramatically, with some vulnerabilities being exploited within hours of public disclosure.

By 2025 we expect AI-driven cyber attacks to become one of the most scalable and adaptable threats, challenging traditional defenses and requiring innovative countermeasures.

In the sections that follow, this report will trace the details of these challenges, vulnerabilities, and emerging trends.

Understanding these intricacies is critical to formulating a defense strategy and mitigating the evolving risks to the digital payments ecosystem.

SHIFT TOWARDS SOCIAL ENGINEERING AND CREDENTIAL THEFT

Social engineering remains one of the most pervasive attack methods in 2024.

Business Email Compromise (BEC)

A notable trend has been the rise of social engineering, with Business Email Compromise (BEC) and sophisticated phishing campaigns dominating the threat landscape. Attackers are increasingly turning to AI-powered tools to mine social media, scrape employee data, and craft highly personalized lures that bypass traditional security filters. Pretexting, the art of creating false scenarios, plays a central role in these attacks, deceiving employees into transferring funds, sharing credentials, or altering account information under the guise of legitimate requests. The growing accessibility of "deepfake as a service" platforms further amplify the effectiveness of these schemes, allowing adversaries to convincingly impersonate executives and bypass manual verification processes.

54% of the Business Email Compromise case investigated had instances of pretexting[4].

Phishing Attacks

Stolen credentials and information stealing malware remain among the most effective tactics for attackers to breach organizational networks. Malicious actors acquire credentials through phishing, information stealing malware, or dark web purchases, targeting usernames, passwords, and session cookies that bypass multi-factor authentication (MFA). These credentials grant access to critical systems like single sign-on platforms, virtual private networks (VPNs), email accounts, and software as a service (SaaS) applications. Many SaaS platforms include client-specific information in URLs, compounding the risk by exposing sensitive data when combined with compromised credentials.

Phishing attacks, accounting for 25% of initial infection vectors, deceive individuals into revealing sensitive information by impersonating trusted entities[5].

IMPACT OF ARTIFICIAL INTELLIGENCE ON CYBER THREATS

Phishing attacks have become increasingly sophisticated with attackers employing advanced social engineering tactics, often enhanced by artificial intelligence (AI), to create highly convincing phishing emails and messages that are difficult to distinguish from legitimate communications. AI's accessibility has democratized cyber attacks, enabling even smaller groups to launch impactful attacks.

The use of AI-generated content to craft phishing lures that are free of grammatical errors and awkward phrasing, which traditionally served as warning signs of malicious intent.

These AI-enhanced phishing attempts can mimic the tone, style, and branding of trusted entities with remarkable accuracy, making them more persuasive and harder to detect.

Further, generative AI models can produce personalized content that exploits specific information about targets, increasing the likelihood of deceiving recipients into revealing sensitive information or clicking on malicious links.

The emergence of malicious Large Language Models (LLMs), such as WormGPT and FraudGPT, has lowered the barrier to entry for sophisticated cyber attacks, enabling less skilled actors to craft convincing phishing emails, generate malware, and exploit vulnerabilities.

The advent of chatbot phishing scams represents a new frontier in phishing techniques. Attackers use AI-powered chatbots with NLP capabilities to engage potential victims in seemingly benign conversations, subtly extracting personal information or login credentials over time. This method leverages the interactive nature of chatbots and can be particularly effective as users may be less guarded during real-time exchanges.

Deepfake-enhanced social engineering attacks are on the rise, with attackers using convincing AI-generated audio and video to impersonate trusted individuals. These advanced impersonations trick users into revealing MFA codes or approving unauthorized authentication requests.

Key Tactics Observed

Diversification of File Formats
Attackers are also diversifying the file formats used in phishing campaigns to evade email security filters. Common tactics include sending malicious attachments in archive formats like ZIP and RAR files, which can conceal harmful content from scanners, especially when password-protected. Additionally, there is increased use of HTML-based files such as Compiled HTML Help (CHM) and LNK (shortcut) files, which are often overlooked by security software due to their legitimate uses.

Abuse of Legitimate Internet Services (LIS)
Attackers exploit services like GitHub Pages, cloud storage platforms, and messaging applications such as Discord and Telegram to lend credibility to their phishing campaigns and to bypass traditional security defenses that trust these well-known platforms.

INCREASE IN SUPPLY CHAIN AND THIRD-PARTY ATTACKS

Supply chain vulnerabilities remained a prominent attack vector for the digital payments industry in 2024. By infiltrating third-party vendors or manipulating widely used software, attackers achieved large-scale breaches. These attacks leveraged trusted relationships to bypass direct defenses, making detection and response increasingly difficult.

In these attacks, the threat actors compromise a product development entity—such as a software vendor or a third-party library provider—to inject malicious code into legitimate applications. This compromised code could be delivered to clients via regular software updates or new releases, allowing attackers to potentially infiltrate multiple organizations without direct targeting.

One prevalent technique is exploiting access to code repositories. Attackers inject obfuscated malicious code into the source code of widely used applications by gaining unauthorized access to developer accounts. This malware can evade detection during automated and manual reviews due to advanced obfuscation techniques.

Another tactic involves publishing malicious libraries disguised as legitimate ones on platforms like GitHub or PyPI. These libraries, promoted to gain developer trust, are unknowingly integrated into projects, introducing vulnerabilities or backdoors.

Key Tactics Observed

Third-Party Exploits

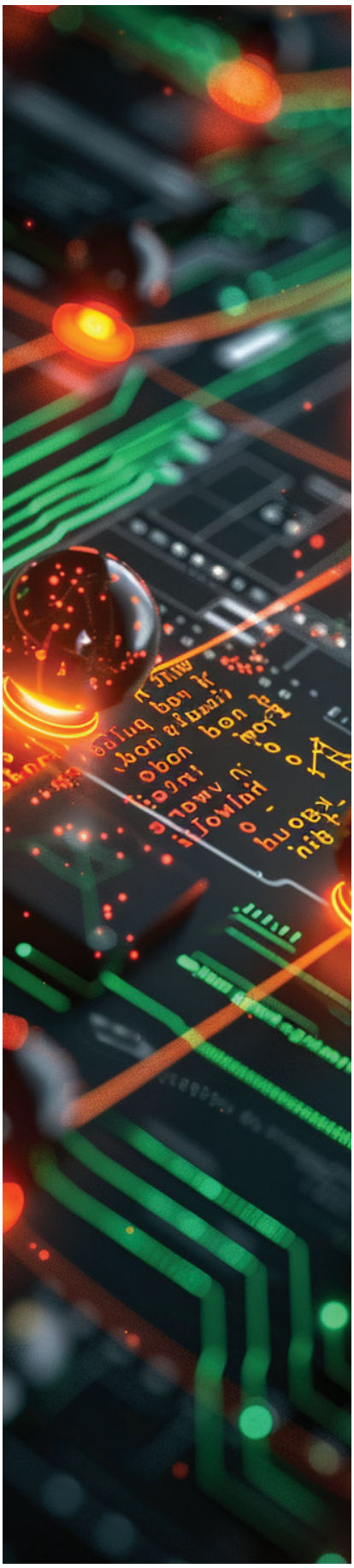
The MOVEit and GoAnywhere breaches highlighted the risks posed by compromised managed file transfer services.

Open-Source Risks

Threat actors exploited vulnerabilities in open-source libraries and components, often targeting Linux environments. For instance, the XZ Utils data compression library was compromised, introducing a backdoor that could have allowed unauthorized access to systems using the library. This incident prompted major Linux distributions to revert to previous, uncompromised versions to mitigate potential risks.

Ransomware Attacks

Threat Actor Groups like CL0P launched attacks on managed file transfer (MFT) services, including Fortra's GoAnywhere and Progress Software's MOVEit, impacting thousands of organizations and exposing sensitive data.



EXPLOITING WEAK LINKS: SECURITY LAPSES AND CLOUD VULNERABILITIES

Organizations with inadequate cloud configurations or insufficient security controls are becoming prime targets for cyberattacks. Common vulnerabilities include poor access controls, lack of multi-factor authentication (MFA), delayed security patches, and mismanagement of privileged accounts.

Cloud misconfigurations—such as publicly accessible storage buckets or default credentials—have led to unauthorized access and massive data exposures. The shift to remote work and the rapid adoption of cloud services have further widened the attack surface, with many organizations failing to recalibrate their security postures to match the speed of digital transformation.

A significant surge has been observed in attackers exploiting vulnerabilities as a primary method to gain initial access into organizational networks. By targeting both known and zero-day vulnerabilities in widely deployed systems and applications, attackers can bypass traditional defenses. These vulnerabilities often affect internet-facing services and can be discovered through public scanning, making them attractive for mass exploitation.

Recent research highlights a 180% increase[6] in exploits leveraging vulnerabilities to infiltrate networks, emphasizing the growing reliance on this tactic. Internet-exposed systems, unpatched software, and misconfigured services present low-hanging fruit for attackers seeking entry points.

However, even organizations with strong security frameworks are not immune. Despite mature security practices, breaches continue to occur, often exploiting subtle vulnerabilities and human error. Sophisticated attackers bypass advanced defenses through social engineering, manipulating trusted insiders to gain unauthorized access.

In a few incidents outside India, it has been observed that super users have been approached with cryptocurrency-based tactics, persuading them to modify security settings, leading to unauthorized access to critical environments.

Attackers exploit flaws within hours of vulnerability's disclosure, with the average time to exploitation now just eight days. This leaves organizations struggling to patch in time.

Application Program Interfaces (APIs) have also become a key attack vector. Weaknesses in API authentication—such as hardcoded API keys, credential reuse across environments, and predictable patterns—are frequently exploited by threat actors. Attackers leverage these gaps to breach systems, often with devastating results.

Furthermore, MFA, once considered a cornerstone of modern security, is increasingly under fire. Attackers bypass MFA through mechanisms such as session hijacking, brute-force attacks on push notifications, and advanced social engineering techniques, including the use of deepfake technology to impersonate trusted individuals. The OTP Bypass via BOLA (Broken Object Level Authentication) is another critical vulnerability which enables malicious actors to bypass authorization mechanisms, granting them unauthorized access to sensitive data or allowing the execution of unauthorized actions.

INSIDE THE BREACH

KEY CYBERSECURITY BREACHES AND ATTACK VECTORS

The evolving cyber threat landscape highlights that no single point of defense is sufficient to protect the intricate and interconnected systems underpinning modern financial services. As adversaries adapt and exploit weak links across digital payments, cloud environments, third-party integrations, and internal processes, BFSI entities must move beyond isolated security measures to adopt a system-level approach to cybersecurity.

Cyberattacks are no longer confined to external breaches or malware infections; they now infiltrate the entire BFSI value chain—from core financial application platforms and payment gateways to cloud infrastructure and customer-facing applications. Supply chain attacks, identity theft, and phishing campaigns are not standalone threats but interwoven tactics that target vulnerabilities across multiple layers of financial services operations. Zero-day vulnerabilities, API exploitation, and social engineering persist as recurring attack vectors, often bypassing traditional security postures by exploiting human error, misconfigurations, or third-party software dependencies.

Recent incidents reveal that no operational domain is immune. BFSI entities have faced ransomware encrypting their systems, low-value unauthorized transactions slipping past payment processing systems, and AI-powered BEC scams exploiting communication channels. Attackers leverage API weaknesses to breach mobile wallets, exploit cloud misconfigurations to access sensitive customer data, and manipulate dormant accounts internally to siphon funds undetected.

To address these challenges, a structured and segmented approach for attack vectors has been adopted to understand the threat actors' tactics. This approach is outlined through eight use cases, each reflecting a unique attack scenario targeting a distinct operational segment of BFSI infrastructure. These cases provide a comprehensive, system-level view of vulnerabilities exploited, attack methods, audit findings and proposed mitigation strategies, illustrating how attackers move fluidly between domains to maximize impact.

STRUCTURED AND SEGMENTED APPROACH FOR ATTACK VECTORS ACROSS THE BFSI OPERATIONS

Core Banking Systems

Ransomware & Data Encryption
Disruption of core banking operations by encrypting databases.

Insider Fraud
Unauthorized manipulation of dormant accounts and transaction records.

Supply Chain Attacks
Malicious code injected via third-party core banking software providers.

Payment Processing Systems

API Exploitation
Weakness in wallet APIs allows unauthorized payments.

MITM (Man-in-the-Middle) Attacks
Transaction data is altered during processing.

Digital Financial Services Apps

App Vulnerabilities
Exploiting mobile app vulnerabilities (XSS, SQL injection) to compromise accounts.

Credential Theft
Phishing and AI-powered scams to steal user login information.

Session Hijacking
Attackers bypass MFA by hijacking active sessions.

Cloud & Infra Management

Cloud Misconfigurations
Public exposure of cloud storage and weak IAM settings.

Privilege Escalation
Gaining admin rights through API vulnerabilities.

Cross-Site Scripting (XSS)
Exploiting web applications hosted in the cloud.

Vendor & Partner Integration Systems

Supply Chain Attacks
Injecting malicious code into third-party banking software.

Third-Party Breaches
Compromising vendor systems to gain access to bank networks.

IoT & Connected Device Security

Hardware Vulnerabilities
Fault injection techniques bypassed security on a Trezor hardware wallet, unlocking $2 million in cryptocurrency.

CASE 1:
THE REWARD HEIST: EXPLOITING SYSTEM VULNERABILITIES FOR FINANCIAL FRAUD

STRUCTURED AND SEGMENTED APPROACH FOR ATTACK VECTORS ACROSS THE BFSI OPERATIONS

Core Banking Systems	Payment Processing Systems
Digital Financial Services Apps	Cloud & Infra Management
Vendor & Partner Integration Systems	IoT & Connected Device Security

This case (outside India) is of a multi-stage cyberattack targeting a reward points system, exploiting server vulnerabilities, and leveraging weaknesses in API transactions for financial fraud.

Attackers breached a Linux web server, exploiting vulnerabilities to deploy malware and secure remote access for themselves. After gaining initial access, the attackers moved laterally within the system by exploiting hardcoded database credentials to access sensitive information. This oversight in database security provided the attackers unrestricted access, allowing them to manipulate critical data.

Attackers targeted the reward points system, inflating the value of 250 points from $50 to $50,000. They updated only specific wallets with these manipulated points, eventually making them universally accessible for redemption and monetization, thus enabling widespread exploitation.

Attackers were able to deceive the system by crediting manipulated reward points to users' mobile wallets. This credit served as a stepping stone for the next phase of the attack which was to transfer funds from mobile wallets to bank accounts. Using a replay attack methodology, they replicated genuine bank transfer requests from physical branches, mimicking API calls with identical request identities to bypass security checks and execute unauthorized transfers.

The attackers' ultimate objective—to inflate reward points, credit unauthorized amounts to wallets, and transfer funds to external accounts—was successfully achieved.

This case underscores significant vulnerabilities, such as the use of hardcoded database credentials, the lack of validation in the reward points system, and the absence of mechanisms to detect replay attacks. It also highlights the importance of robust vulnerability management, secure transaction workflows, and continuous monitoring to prevent such exploitation.

Top 5 Mitigation Steps

1. **Multi-Factor Authentication (MFA):** Enable MFA for VPNs, webmail, and accounts accessing critical systems.
2. **Network Segmentation:** Segment and segregate networks into security zones, separating administrative networks from business processes using physical controls and virtual local area networks (VLANs).
3. **Application Whitelisting:** Enforce whitelisting on endpoints to block unauthorized software execution.
4. **Log Monitoring and Retention:** Audit and monitor logs to detect unusual patterns or behaviors in events and incidents. Redesign log retention policies to store logs for at least 180 days to ensure availability for incident investigations.
5. **Regular Updates and Virtual Patching:** Ensure all operating systems and applications are updated regularly. Use virtual patching to protect legacy systems and networks.

CASE 2:

THE SILENT HEIST : LOW-VOLUME FRAUD TARGETING SMALL ENTITIES IN BFSI SECTOR

STRUCTURED AND SEGMENTED APPROACH FOR ATTACK VECTORS ACROSS THE BFSI OPERATIONS

Core Banking Systems	**Payment Processing Systems**
Digital Financial Services Apps	Cloud & Infra Management
Vendor & Partner Integration Systems	IoT & Connected Device Security

CSIRT-Fin/CERT-In has been watchful and has proactively taken measures and thwarted cyber-attacks which could have caused damage in the BFSI sector.

But for the timely intervention and preventive measures, any lapses would have resulted in financial and reputational risk for the sector.

Small entities in the BFSI sector must take proactive steps to secure their information system infrastructure against cyber-attacks.

The attackers aimed to bypass security checks and exploit gaps in the information infrastructure of these small entities. Key protective measures include enforcing Multi-Factor Authentication (MFA), segmenting networks into secure zones, implementing application whitelisting, using virtual patching for legacy systems, and deploying robust web and email filters with antivirus scanning at both host and gateway levels.

Top 5 Mitigation Strategies

1. **Multi-Factor Authentication (MFA):** Enforce MFA for accessing critical systems.
2. **Network Segmentation:** Segment and segregate networks into security zones to protect sensitive information and services.
3. **Application Whitelisting:** Enforce whitelisting on endpoints to prevent unauthorized software execution.
4. **Virtual Patching:** Use virtual patching to safeguard legacy systems and networks.
5. **Deploy Filters:** Implement web and email filters to block known malicious domains, sources, and addresses. Scan all emails, attachments, and downloads with a reputable antivirus solution at both host and gateway levels.

CASE 3:
THE SILENT INFILTRATION: RANSOMWARE THROUGH THE CORE BANKING SUPPLY CHAIN

STRUCTURED AND SEGMENTED APPROACH FOR ATTACK VECTORS ACROSS THE BFSI OPERATIONS

Core Banking Systems	Payment Processing Systems
Digital Financial Services Apps	Cloud & Infra Management
Vendor & Partner Integration Systems	IoT & Connected Device Security

A third-party service provider in the BFSI sector was impacted by a cyber attack.

The attacker, a member of the notorious RansomEXX ransomware group, gained access through vulnerabilities in the provider's infrastructure, slipping past defenses undetected.

This wasn't a direct assault on the BFSI entity—but rather an exploitation of the supply chain that underpinned the entity's core services.

Once inside, the attacker deleted critical database backups and deployed a custom ransomware variant called 'cryptor', encrypting critical files. The ransom note left behind was more than just a demand—it was a threat of double extortion, warning that sensitive client data would be leaked if the ransom wasn't paid. (Double extortion – (1) demand for ransom, (2) leaking client data)

The compromised entity suffered reputational damage, operational disruption, and an increased risk of customer churn.

Top 5 Mitigation Strategies

1. **Multi-Factor Authentication (MFA):** Enable MFA for VPNs, webmail, and accounts accessing critical systems.
2. **Regular Updates:** Ensure all operating systems and applications are updated regularly. Use virtual patching to protect legacy systems and networks.
3. **Data Protection:** Enforce data protection, backup, and recovery measures. Encrypt data at rest to safeguard against breaches and exfiltration.
4. **Advanced Security Systems:** Deploy intrusion detection & prevention systems, network detection and response system, extended detection and response system, network behaviour and anomaly detection system, and firewalls as appropriate for enhanced threat detection and prevention.
5. **Network Segmentation:** Implement network segmentation into security zones. Separate administrative networks from business processes using physical controls and VLANs.

CASE 4:

THE WALLET EXPLOIT: BREACHING PAYMENT SYSTEMS THROUGH VULNERABLE WALLET FLOWS

STRUCTURED AND SEGMENTED APPROACH FOR ATTACK VECTORS ACROSS THE BFSI OPERATIONS

Core Banking Systems	Payment Processing Systems
Digital Financial Services Apps	Cloud & Infra Management
Vendor & Partner Integration Systems	IoT & Connected Device Security

In a carefully orchestrated attack on a payment service entity, the threat actors exploited a vulnerability in the wallet flow of the payment service entity, targeting the integration between the payment service provider and merchants, to carry out multiple unauthorized transactions.

By leveraging this exploit, the attackers seamlessly placed orders through third-party applications, exploiting the direct link between the payment service provider and external merchants. The loophole created a perfect storm—transactions appeared valid on the merchant's side while leaving the actual wallet balances untouched.

The payment service provider faced financial losses. Subsequently this vulnerability has been fixed.

Top 5 Mitigation Strategies

1. **Confidentiality:** Restrict access to API documentation, including Postman collections, ensuring it is accessible only to authorized personnel.
2. **Strong Authentication:** Use robust mechanisms like API keys, OAuth, or JSON web token (JWT) with secure token management practices, appropriate expiration times, and granular access control based on user roles and permissions.
3. **Multi-Factor Authentication (MFA):** Enable multi-factor authentication of users particularly for accounts that access critical systems.
4. **Secure Storage:** Encrypt and secure API keys, credentials, and sensitive data with access controls.
5. **Cross-Origin Resource Sharing (CORS) Configuration:** Properly configure CORS to restrict API access to specific domains, preventing unauthorized cross-origin requests.

CASE 5:

THE CASHBACK MANIPULATION: EXPLOITING PAYMENT SYSTEMS THROUGH TRANSACTION INTERCEPTION

STRUCTURED AND SEGMENTED APPROACH FOR ATTACK VECTORS ACROSS THE BFSI OPERATIONS

Core Banking Systems	**Payment Processing Systems**
Digital Financial Services Apps	Cloud & Infra Management
Vendor & Partner Integration Systems	IoT & Connected Device Security

A digital payments and financial services company fell victim to a sophisticated man-in-the-middle (MITM) attack that exploited the intricacies of an instant cashback promotion tied to EMI purchases on an e-commerce platform.

By intercepting and altering transaction details midstream, the attacker systematically inflated cashback values, bypassing essential verification steps. This allowed the perpetrator to successfully claim cashback rewards.

The lack of real-time validation or API integrity checks facilitated the attack's longevity, resulting in unauthorized cashback claims.

This breach not only inflicted direct financial losses but also exposed systemic vulnerabilities in the payment service entity's API security and transaction validation mechanisms.

Top 5 Mitigation Strategies

1. **API Security:** Secure APIs used between the merchant's website, payment aggregator, payment gateway, and acquirer with strong authentication, encryption, and access controls.
2. **Server-to-Server Validation:** Use server-to-server validation techniques instead of browser redirection or callbacks for enhanced security.
3. **Hash Sensitive Details:** Include sensitive payment details like card numbers, transaction amounts, and statuses in the hash or checksum transmitted with transaction data.
4. **Real-Time Monitoring:** Implement monitoring and anomaly detection systems to identify unusual patterns or potential security incidents in real time. Set up alerts for security threats.
5. **Encrypt Payment Data:** Protect stored payment data with strong encryption algorithms to prevent unauthorized access.

CASE 6:
THE WEBSHELL BREACH - EXPLOITING XSS TO INFILTRATE CLOUD INFRASTRUCTURE

STRUCTURED AND SEGMENTED APPROACH FOR ATTACK VECTORS ACROSS THE BFSI OPERATIONS

Core Banking Systems	Payment Processing Systems
Digital Financial Services Apps	**Cloud & Infra Management**
Vendor & Partner Integration Systems	IoT & Connected Device Security

A fintech company specializing in tax related services became the target of a sophisticated cyberattack that exposed critical weaknesses in its cloud infrastructure. The breach began with the exploitation of cross-site scripting (XSS) in a commonly used rich text editor embedded in the company's web applications.

The attacker used the XSS vulnerability to inject malicious scripts, establishing a foothold within the company's environment. From there, the threat actor escalated access, deploying webshells (enables a threat actor to remotely access the web server) to execute commands directly on the company's Amazon Web Services (AWS) infrastructure. By leveraging these webshells, the attacker gained unauthorized access to the company's Simple Storage Service platform (S3 bucket), where sensitive client data was stored.

This unauthorized access led to a severe data breach, operational disruption, and financial losses. Client trust eroded as sensitive financial records and business data were compromised, highlighting the cascading impact of inadequate web application security combined with cloud misconfigurations.

Top 5 Mitigation Strategies

1. **Multi-Factor Authentication:** Enable multi-factor authentication of users particularly for cloud, virtual private networks, webmail, and accounts that access critical systems.
2. **Cloud Instance Security:** Check public accessibility of all cloud instances in use. Make sure that no server/bucket is inadvertently leaking data due to inappropriate configurations.
3. **Access Token Security:** Ensure proper security of AWS/Azure/GCP access tokens. The tokens should not be exposed publicly in website source code, any configuration files, etc.
4. **Data Protection and Encryption:** Enforce data protection, backup, and recovery measures. Encryption of the data at rest should be implemented to prevent the attacker from accessing the unencrypted data in cases of data breaches/exfiltration.
5. **Least Privilege Access Control:** Implement least privilege principle for access control with granular permission to cloud resources.

CASE 7:

THE INSIDER THREAT: MANIPULATING DORMANT ACCOUNTS FOR FINANCIAL GAIN

STRUCTURED AND SEGMENTED APPROACH FOR ATTACK VECTORS ACROSS THE BFSI OPERATIONS

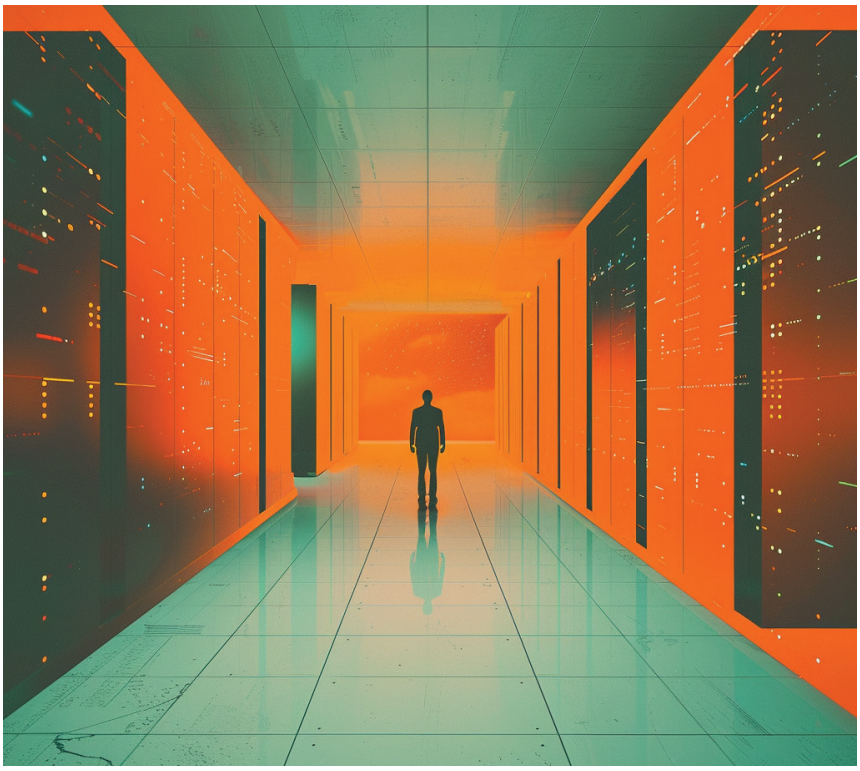
Core Banking Systems	Payment Processing Systems
Digital Financial Services Apps	Cloud & Infra Management
Vendor & Partner Integration Systems	IoT & Connected Device Security

An insider threat case (outside India) reveals how an employee abused administrative privileges to manipulate dormant accounts and withdraw funds undetected. With access to critical systems, the insider threat actor orchestrated financial pilferage over a period of two years.

The insider exploited dormant accounts in the system, using administrative access to request for prepaid cards linked to these accounts. By altering address details, the insider redirected the cards to itself, bypassing original account holders.

Post receiving the prepaid cards, the perpetrator manipulated the database to inflate account balances, loading the cards with substantial funds. The withdrawal of the money was via ATMs, concealing the modus operandi by deleting transaction data and restoring balances to erase all traces.

To maintain persistence, the perpetrator created misleading root cause analysis (RCAs) for unauthorized transactions. The investigations were misdirected ensuring the cover up continued undetected for two years.



Top 5 Mitigation Strategies

1. **Least Privilege Principle:** Apply the principle of least privilege across all system levels to minimize risk. Limit administrative access to critical systems and enforce strict role-based access controls (RBAC).
2. **Log Retention and Monitoring:** Redesign log retention policies to store logs for at least 180 days. Continuously audit and monitor logs to detect unusual patterns or unauthorized access to dormant accounts.
3. **Multi-Factor Authentication (MFA):** Enforce MFA for accessing critical systems. Mandate MFA for remote access to prevent unauthorized administrative actions.
4. **Regular Security Audits:** Conduct regular security audits of internal systems and databases through CERT-IN empaneled auditors. Regularly review and reconcile dormant accounts to detect and prevent unauthorized manipulation.
5. **Application Whitelisting and Network Segmentation:** Enforce application whitelisting on endpoints to block unauthorized software execution. Segment networks to restrict administrative access to specific zones, ensuring that sensitive systems are isolated from broader environments.

SECURING THE EXPANDING IoT FRONTIER IN BFSI: A GROWING IMPERATIVE

The Internet of Things (IoT) is transforming the way businesses operate, particularly in industries driven by digital innovation such as Banking, Financial Services, and Insurance (BFSI). IoT has embedded itself into daily workflows, revolutionizing customer experiences and streamlining operations. From connected ATMs to wearable payment devices, the integration of IoT in financial services has redefined engagement, data collection, and service delivery.

The number of Internet of Things (IoT) devices worldwide is forecast to reach 32.1 billion IoT devices in 2030, significantly broadening the attack surface. As IoT adoption accelerates, financial institutions are increasingly relying on these devices to optimize processes and enhance customer interactions. However, with this exponential growth comes an alarming rise in security vulnerabilities. Nearly 99% of IoT exploitation attempts leverage previously known vulnerabilities (CVEs), exposing critical gaps in security infrastructure.

Financial institutions are increasingly leveraging IoT for personalized services. Banks utilize IoT to identify and greet customers as they enter branches, enhance credit risk assessments through real-time data, and deliver targeted product recommendations via wearables. IoT-powered devices also facilitate on-the-go transactions and enable remote account opening through smart speakers and mobile devices. These advancements not only enrich customer experiences but also provide valuable insights into consumer behavior.

However, in the BFSI sector, IoT applications extend beyond front-end customer interactions. Check scanners, touch-enabled kiosks, branch digital signage, and bluetooth beacons silently operate behind the scenes, enhancing user engagement and operational efficiency. On-premise ATMs interface with connected devices, amplifying potential vulnerabilities.

A key challenge in securing IoT in financial services is visibility and control—knowing where devices are deployed and how they operate. Forrester's research highlights that 36% of financial leaders prioritize IoT-driven operational efficiency. Yet, many IoT deployments in banking, trade finance, and supply chain management often lack adequate oversight. This lack of visibility leaves financial ecosystems exposed to potential breaches and cyberattacks.

The consequences of IoT vulnerabilities are significant. Forrester's findings reveal that 34% of enterprises impacted by IoT breaches experienced losses ranging from $5 million to $10 million—substantially higher than attacks on traditional IT infrastructure.

The last case is an in-depth analysis that explores IoT vulnerabilities and attacks, providing valuable insights into how these risks translate to the BFSI sector. By examining real-world incidents—from breaches through connected fish tanks and medical devices to compromised home security cameras and cryptocurrency wallets—this analysis underscores the critical need for enhanced IoT security measures.

CASE 8:
TURNING A $2 MILLION HACK INTO A HARDWARE-HACKING MILESTONE

STRUCTURED AND SEGMENTED APPROACH FOR ATTACK VECTORS ACROSS THE BFSI OPERATIONS

Core Banking Systems	Payment Processing Systems
Digital Financial Services Apps	Cloud & Infra Mgmt
Vendor & Partner Integration Systems	**IoT & Connected Device Security**

Hardware hacker Joe Grand successfully unlocked a Trezor wallet (outside India) containing US$2 million in cryptocurrency by exploiting hardware vulnerabilities through fault injection[7].

Faced with strict PIN limits and irreversible data erasure, Grand used voltage glitching to disrupt the wallet's boot process, bypassing the Readout Protection (RDP) mechanism. By precisely inducing a "brown-out" during the boot process, Grand disrupted the firmware's security check, forcing the Trezor to copy the unencrypted seed and PIN into RAM—allowing him to extract them without triggering the system's safeguards.

The attack required precise manipulation—removing capacitors, fine-tuning glitch parameters, and avoiding crashes that could erase critical data. Careful tuning of signal widths, wire lengths, and trigger points proved essential in hitting the microcontroller at exactly the right moment. After hours of meticulous attempts, Grand successfully retrieved the funds, demonstrating how microcontroller weaknesses in embedded devices can be exploited if not rigorously secured against fault attacks.

Mitigations Steps to Prevent Hardware Wallet Hacks

Strengthen Hardware and Physical Security

Ensuring the physical security of hardware wallets is paramount to prevent unauthorized access and tampering. Implementing tamper detection systems that trigger automatic data wipes if tampering is detected can significantly reduce risks. Additionally, employing tamper-evident and tamper-resistant packaging serves as a deterrent against physical breaches. By isolating critical components and restricting physical access to sensitive areas, attackers are further hindered from exploiting vulnerabilities. Secure microcontrollers with built-in protections provide another layer of defense, making unauthorized physical access extremely challenging.

Enhance Fault Injection and Debugging Protections

One of the most effective ways to prevent hardware hacks is by implementing robust fault injection countermeasures. Fault injection attacks exploit vulnerabilities by disrupting normal hardware operations, allowing attackers to bypass security mechanisms. Strengthening Readout Protection (RDP) levels and securely locking or disabling debug interfaces in production environments is crucial to thwart such attacks. Debug interfaces are often exploited to access sensitive data or manipulate firmware, so securing them from the outset ensures a more resilient device.

Ensure Secure Boot and Trusted Firmware

The boot process represents a critical attack surface, making it essential to secure boot processes with verified bootloaders. Utilizing a Hardware Root of Trust (HRoT) ensures that only authorized and verified firmware is loaded during the boot process, preventing malicious code injections. Encrypting sensitive data in RAM and minimizing exposure during the boot sequence further reduces the attack surface. By ensuring that each layer of the boot process is authenticated, potential attackers are unable to manipulate firmware or introduce vulnerabilities at the boot / startup time.

Mitigate Side Channel and Memory-Based Attacks

Side channel attacks (SCA) can extract sensitive information by analyzing power consumption, electromagnetic leaks, or timing information. Implementing protections against side channel attacks and continuously evaluating device security through SCA simulations is critical. Encrypting sensitive data stored in RAM and employing secure communication protocols during data exchanges adds further resilience against potential memory extraction attacks. This layered approach minimizes the risk of data leakage even if parts of the device are compromised.

Continuous Monitoring and Security Audits

Regularly updating and patching firmware ensures that vulnerabilities are addressed promptly, reducing exposure to newly discovered threats. Comprehensive hardware security audits help identify weaknesses in the device's design and implementation, allowing for pre-emptive mitigations. Additionally, employing secure communication protocols during data exchanges ensures that sensitive information remains encrypted in transit. By establishing a cycle of continuous improvement through audits, patches, and updates, hardware wallets remain resilient against evolving attack techniques.

REGULATORY FOCUS: A SPECIAL FEATURE

2025 AND BEYOND: NAVIGATING EVOLVING REGULATIONS IN THE DIGITAL PAYMENTS LANDSCAPE

As we move into 2025, the digital payments and BFSI industries stand at the cusp of a transformative shift driven by regulatory changes and the accelerating digitization of financial services.

In this shifting landscape, compliance is no longer merely a matter of adhering to checklists but has emerged as a strategic imperative that will shape the industry's future. This transformation is not without its challenges, but it also opens a gateway to significant opportunities for growth and resilience.

The rapid pace of regulatory evolution has created a complex environment for financial institutions. Mandates such as CERT-IN directives for reporting cyber incidents within 6 hours of noticing such incidents or being brought to notice about such incidents, RBI Master Direction in Digital Payment Security Controls(DPSC) and Master Direction in Outsourcing of Information technology services; RBI Cyber Security Framework in Banks (CSF); SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF), Digital Personal Data Protection (DPDP) Act, 2023, PCI DSS 4.0, European General Data Protection Regulation (GDPR),the California Consumer Privacy Act (CCPA) have set new benchmarks for accountability and data protection. These frameworks underscore the urgent need for organizations to anticipate and adapt to emerging risks, especially as the digital payments sector, with its vast repository of sensitive financial data, becomes an increasingly attractive target for cyber perpetrators. However, the fragmented nature of compliance frameworks across jurisdictions adds another layer of complexity, particularly for businesses operating across borders. Local laws, cultural nuances, and jurisdictional variations often result in inefficiencies, especially in cross-border payment solutions, which are crucial to the financial industry's global operations.

Despite these hurdles, the narrative is beginning to shift toward regulatory harmonization.

The push for unified global standards is gaining momentum, offering a way to bridge regional gaps and create cohesive frameworks that simplify compliance and improve operational efficiency.

This movement toward regulatory alignment is not just a means of reducing friction but hold the promise of making compliance an enabler of growth for the financial sector globally.

The dual demands of regulatory compliance and technological innovation present a delicate balancing act for digital payment organizations. The need to stay ahead in areas such as real-time payments, fraud detection, and predictive financial services requires a forward-looking approach to compliance. Emerging techniques like data anonymization and synthetic data generation are paving the way for innovation without compromising privacy or security. Additionally, embedding compliance into the design phase of new technologies is proving to be a game-changing strategy, enabling organizations to future-proof their innovations and mitigate risks proactively.

The integration of compliance and innovation is not merely a response to external pressures but a fundamental shift in how organizations view their roles in the digital ecosystem. The expected growth of cyber attacks underscores the critical need for resilience and adaptability. In this context, compliance is no longer seen as a cost center but as a cornerstone of trust and a catalyst for growth. It has become an essential component of an organization's ability to build credibility and foster long-term customer loyalty.

As the BFSI industry moves forward, the conversation around compliance is evolving. What was once perceived as a reactive, burdensome process is now recognized as a strategic driver of resilience and innovation. The ability to navigate a harmonized compliance framework will not only help organizations manage the growing complexity of regulatory requirements but also position them to thrive in an interconnected, data-driven global economy. The next decade will redefine the role of compliance, transforming it into a force that propels the industry toward greater trust, innovation, and sustainable growth.

RBI, IRDA and SEBI are proactively supporting the BFSI sector from a policy and direction perspective, CERT-In and CSIRT-Fin are helping from a strategic, tactical and operational perspective. Thus, all these entities are working cohesively to ensure trust and resilience in the BFSI sector for all stakeholders.

SUGGESTIONS TO POLICY MAKERS

Cybersecurity should be a techno-commercial business decision and not just decided only on commercials

Cybersecurity investments must be driven by a balance of technical requirements and commercial viability. Prioritizing security as a strategic enabler ensures resilience, robust protection against threats, safeguarding business continuity and customer trust.

Empower CISOs through direct reporting to the CEO/CRO instead of CTO or CIO

Granting Chief Information Security Officers (CISOs) direct access to top leadership enables better alignment of cybersecurity strategies with business goals, ensuring accountability and a stronger focus on organizational risk management.

Digital Payment Security to have common standards for all Digital Payment Form Factors

Harmonizing security standards across all digital payment methods—not just cards—ensures a consistent and comprehensive security framework that addresses emerging risks in alternative payment systems like wallets, UPI, and QR codes.

Create more Certified Digital Payment Security Specialists in the ecosystem

Addressing the talent gap requires fostering a skilled workforce through certification programs focused on payment security. This will enable enterprises to design secure payment applications and implement robust security standards effectively.

Clear Preparation Roadmap for Post-Quantum Cryptography

Policymakers must prioritize developing a strategic roadmap to transition to quantum-resistant cryptography, ensuring businesses are prepared for future threats posed by quantum computing advancements.

Building a Responsible AI Framework for BFSI

To ensure the responsible deployment of AI and ML in the banking and financial services industry, policymakers must implement clear, comprehensive regulations that balance innovation with consumer protection and system stability. Providing the industry with clear guidelines around critical aspects such as data privacy, ethical AI use, and algorithmic transparency will encourage responsible AI adoption, supporting growth while safeguarding the integrity of the financial sector and protecting consumer interests.

SISA

certin
Enhancing Cyber Security in India

CSIRT-Fin

INSIGHTS ACROSS LAYERS OF DEFENSE SEEN IN BFSI SECTOR

Now that we've explored advanced threats and exploitation techniques, let's examine the compliance levels based on sampled entities in the BFSI sector.

Cybersecurity today mirrors Einstein's notion of insanity—relying on the same strategies and expecting different outcomes. Despite increasing investments in security technologies, breaches remain frequent.

Consider this: Gartner projects worldwide end-user spending on information security to reach US$212 billion by 2025, marking a 15.1% increase from 2024. While this reflects the growing importance placed on cybersecurity, it also underscores a concerning trend: the more we spend, the more sophisticated and widespread attacks become. This paradox isn't merely about advanced threat actors; it's also about foundational cracks in how organizations approach cybersecurity.

For instance, the average organization deploys an astonishing 64-76 cybersecurity tools[8], yet breaches do occur. Why? Because the solution isn't simply about spending more money or adding more tools. Resilience cannot be achieved through isolated efforts. Both organizations with weak security postures and those with robust defenses face significant risks, emphasizing the need for continuous vigilance, proactive measures, and alignment between compliance and security. Achieving resilience requires continuous threat visibility, proactive defense strategies, continuous training & awareness of the work force, robust processes and a security-first mindset that uses compliance frameworks as a foundation.

In the next section, we decode the domains where further improvements are needed.

HEADING	CONTROL	% COMPLIANT IN INDIA	% COMPLIANT GLOBAL
System Hardening and Configuration Management	Hardening and configuration documentation aligned with Center for Internet Security (CIS) standards	🟢	🟢
System Hardening and Configuration Management	Configuration standard and baseline document maintenance	🟢	🟢
Data Protection and Encryption	Encryption of cardholder data and masking of sensitive information	🟢	🟢
Data Protection and Encryption	Use of tokenization or TDE (Transparent Data Encryption) for sensitive data	🟢	🟢
Access Control and User Management	User access lists for Cardholder Data Environment (CDE) and privileged access controls	🟢	🔴
Patch and Vulnerability Management	Timely application of patches and adherence to vulnerability management procedures	🟠	🟠
Intrusion Detection and Prevention	IDS/IPS configurations to detect and prevent unauthorized access	🟢	🟠
Network Security and Segmentation	Network segmentation to isolate CDE and prevent lateral movement	🟢	🟢
Authentication and Password Management	Multi-factor authentication (MFA) and password configuration policies	🟢	🟢
Log Monitoring and Event Management	Centralized logging and monitoring of failed logins and access attempts	🟢	🟢
Incident Response and Contingency Planning	Defined incident response procedures and contingency planning	🟢	🔴
Regular Testing and Vulnerability Scanning	Regular internal and external vulnerability scans and penetration testing	🔴	🟢

🟢 **Manageable** 🟠 **Needs Improvement** 🔴 **Major Concern**

METHODOLOGY FOR DETERMINING COMPLIANCE PERCENTAGES (FOR INDIA & GLOBAL)

Assessment Scope

SISA assessed approximately 1,550 clients globally between November 2022 and November 2024 to derive the observed control gap compliance percentages.

Data Sources

The analysis is based on technical gap reports generated from assessments conducted by SISA's Qualified Security Assessors (QSAs).

Standards Covered

The gap assessments included PCI DSS, PCI PIN, P2PE, PCI SAQ, and local governance standards and regulations.

India-Specific Calculation

Out of 850 clients assessed in India, 765 were compliant while frequently encountering observed control gaps.

Global Calculation

A similar methodology was applied to 700 clients assessed outside India to determine global compliance percentages.

EVALUATING SECURITY MATURITY: TECHNICAL TRENDS AND GAPS IN THE BFSI SECTOR

The security posture of financial institutions audited/reviewed across various domains demonstrates a mixed level of compliance and maturity in critical security areas. Here's a breakdown of key trends and gaps observed across different security layers in the BFSI sector:

Perimeter Security/Network Security

Firewall: Most institutions have implemented basic firewall configurations, however, clients allow all traffic through open policy configurations, lacking granular control. Additionally, insufficient impact analysis in change management processes leads to critical changes not being tracked, increasing the risk of unauthorized access.

DDoS Mitigation: DDoS protection is largely limited to internet service provider (ISP)-level solutions, and dedicated enterprise-grade DDoS mitigation is often missing. This leaves institutions vulnerable to volumetric and application-layer attacks.

Content Filtering / Proxy: Similar to application security, network-level content filtering shows a lack of dedicated solutions and regular reviews, which are essential for filtering malicious or unwanted traffic.

Email Gateway: Email gateways primarily use standard Domain-based Message Authentication, Reporting, and Conformance (DMARC), and Sender Policy Framework (SPF) configurations. However, geo-location-based blocking and periodic rule reviews are often missing, which weakens phishing and spam defences.

Virtual Network / Network Segregation: Many institutions have implemented network segmentation but often lack proper testing and validation of these segmentation controls. Overly broad access control mechanisms are frequently observed, which undermines the intended security benefits of segmentation.

Application Security

IPS/IDS: There is a fair presence of Intrusion Prevention and Detection systems. However, medium and low severity signatures often remain unblocked, and many organizations lack internal IPS, posing risks to application security.

Content Filtering / Proxy: This area lacks dedicated solutions and consistent rule reviews. Absence of content control increases exposure to unfiltered, potentially malicious traffic.

Web Application Firewall (WAF): WAF implementation is inconsistent. Many applications are not covered, and URI paths are not adequately tested or blocked. High and medium threat signatures are often set only to detect, leaving gaps in active defences.

Secure Configuration

Webserver & Database: Lack of application hardening and limited security standards in application design, coupled with inadequate coordination between security and application teams, results in a larger attack surface and greater exposure to vulnerabilities.

Cloud Security

General Cloud Security: Cloud environments show significant gaps. Subscriptions often lack hardening per CIS or global standards, with MFA and logging not enabled by default. Local accounts, sometimes exposed to the internet, increase risk of unauthorized access.

Cloud Environment Specifics (AWS, Azure, GCP): Common gaps include missing audit logging for PaaS, insufficient hardening, and absent MFA. These vulnerabilities reflect a need for stronger cloud access control and monitoring.

Monitoring & Response

Security Logging: Critical logs such as DNS, proxy, MFA, and O365 (email logs) are not integrated by many organizations. This lack of integration limits visibility and hampers the ability to detect potential threats effectively. Additionally, API-based integrations for SAAS services are sometimes constrained by licensing limitations, further impacting comprehensive threat monitoring.

SIEM Integration: SIEM integration lacks comprehensive data feeds, such as DNS and MFA logs, essential for threat correlation. This hinders timely detection and response capabilities, particularly for SAAS and cloud environments.

IAM (Identity and Access Management) Security

Identity Security: Identity security remains a crucial gap. MFA is not universally enforced on VPN profiles, and conditional access policies are missing in a majority of environments, which increases susceptibility to unauthorized access.

User Access review: If excessive user rights are not revoked or accounts for all terminated users have not been removed in due time, they may be used by malicious users for unauthorized access.

Endpoint Security

Endpoint Detection and Response (EDR): Most large financial institutions have implemented EDR solutions, providing advanced detection and response capabilities. However, some mid-sized and smaller clients are still relying primarily on traditional antivirus (AV) solutions with limited EDR functionality. This limits the scope of endpoint threat containment and makes them more vulnerable to sophisticated attacks that require proactive threat hunting and automated response.

Data Protection and Encryption

Encryption of data and masking sensitive information – Sensitive and confidential data is not stored in encrypted form or masked leading to a breach of confidentiality of stored data. Non-compliance to this control may lead to malicious entity to derive the sensitive data.

VAPT (Vulnerability Assessment and Penetration Testing)

Internal/External vulnerabilities and Penetration testing – Periodic vulnerability management and penetrations testing are not regularly followed by many financial institutions. Attackers routinely look for unpatched or vulnerable externally facing servers, which can be leveraged to launch a directed attack. Because external networks are at greater risk of compromise, external vulnerability scanning must be performed periodically.

GAZING THROUGH THE CRYSTAL BALL FOR 2025

GAZING THROUGH THE CRYSTAL BALL FOR 2025

Before we dive into recommendations based on the gaps and vulnerabilities highlighted in the previous section, it's crucial to shift our focus forward and grasp how the cybersecurity landscape is set to transform in the coming year. Understanding the trends and challenges of 2025 is not just valuable—it's imperative for crafting strategies that are resilient to the threats of tomorrow.

As we peer into the future of cybersecurity, the crystal ball reveals a landscape dramatically reshaped by the power of artificial intelligence. Attacks in 2025 will not only be more sophisticated but also exponentially more evasive and pervasive. Threat actors are set to harness AI to craft highly customized assaults, leaving minimal trace as they operate at an unprecedented scale—powered by the same revolutionary technologies transforming industries globally. Add to that the looming quantum computing revolution capable of rendering today's encryption obsolete, organizations face an evolving and complex reality. Preparing for these seismic shifts is no longer optional; it's essential for survival.

Drawing insights from observed threats across the digital payment ecosystem, we present a series of predictions for 2025 - seven highly anticipated attack methodologies likely to dominate the threat landscape in 2025.

These insights aim to empower organizations with a forward-looking perspective, guiding them to anticipate, adapt, and fortify their defenses in the face of an increasingly volatile cyber environment.

ANTICIPATED ATTACK 1:
RISE OF DEEP FAKES AND AI-GENERATED CONTENT

Attackers are expected to increasingly leverage deep fakes and AI-generated content as potent tools for intrusion, particularly in social engineering attacks. The advancement of deep fake technology enables the creation of highly realistic and manipulated audio and video content that can convincingly impersonate individuals.

Deep fake voice and video allow cyber perpetrators to mimic the voices and appearances of executives, employees, or trusted partners. For example, an attacker might use a deep fake video during a virtual meeting to deceive a finance team into authorizing a unauthorized transfer or employ a deep fake voice to trick individuals into revealing one-time passwords (OTPs) for multi-factor authentication (MFA), passwords, or other sensitive information.

The challenges in detection and verification of such AI-generated content are significant. As the technology becomes more sophisticated and accessible, it becomes increasingly difficult for users to distinguish between genuine and manipulated media. Traditional verification methods that rely on voice recognition or visual confirmation are no longer sufficient, as deep fakes can replicate these cues with high accuracy. This creates substantial risks, especially in business contexts where critical decisions and transactions are made based on virtual interactions.

ANTICIPATED ATTACK 2:
GROWING THREAT OF SUPPLY CHAIN ATTACKS AND MALICIOUS LIBRARIES

Attackers are expected to increasingly focus on supply chain attacks, exploiting vulnerabilities in software development processes to compromise multiple organizations simultaneously. One primary method involves the exploitation of code repositories. Cyber attackers gain unauthorized access to developers' accounts on platforms like GitHub or inject malicious code into the source code of widely used applications. By infiltrating the development environment, attackers can insert malware directly into the codebase, which is then unknowingly distributed to clients through regular software updates or new releases. This tactic enables attackers to bypass traditional security measures, as the malicious code originates from a trusted source.

Another concerning trend is the distribution of malicious libraries disguised as genuine. Attackers publish counterfeit libraries that mimic legitimate ones, often with names that are deceptively similar to popular libraries.

Unsuspecting developers may inadvertently incorporate these tainted libraries into their projects, introducing vulnerabilities, backdoors, or malware into their applications. This method allows attackers to spread malicious code across a wide array of software products and services, amplifying the potential impact.

Furthermore, there is growing apprehension about the influence on Large Language Models (LLMs). Attackers may attempt to manipulate LLMs or their training data to promote malicious libraries. By poisoning the datasets or exploiting vulnerabilities in the models, they can cause LLMs to suggest or generate code that includes compromised libraries. Developers relying on LLMs for coding assistance or recommendations might then integrate these malicious components into their applications, unknowingly propagating vulnerabilities. Even in organizations that prohibit direct use of LLM-generated code, developers may still seek guidance from these models, increasing the risk of incorporating tainted libraries.

ANTICIPATED ATTACK 3:
EMERGING THREAT OF LLM PROMPT HACKING IN APPLICATIONS

As Large Language Models (LLMs) become increasingly integrated into various applications, there is a growing threat of LLM prompt hacking, where attackers manipulate the inputs to these models to induce unintended and potentially harmful behaviors. This threat is particularly pronounced in applications that host LLMs locally, rather than relying on APIs from established providers like OpenAI or Anthropic.

Locally hosted LLMs may lack the comprehensive safety measures and robust security features implemented by these providers, making them more susceptible to exploitation.

Vulnerabilities in Locally Hosted LLMs

When organizations incorporate LLMs directly into their environments, they assume the responsibility for implementing security measures to protect against prompt hacking and other attacks. Many locally hosted LLMs may not have sufficient safeguards against adversarial inputs, leaving them vulnerable.

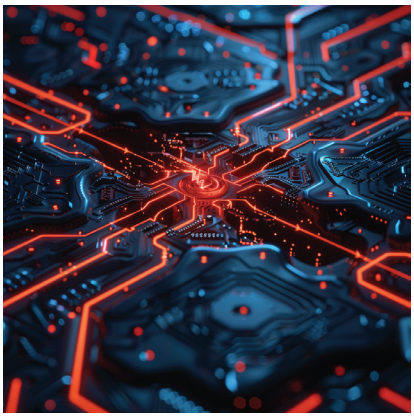
Attackers can exploit these vulnerabilities to manipulate the LLM's output, leading to unauthorized actions, disclosure of sensitive information, or the generation of harmful content.

Prompt Hacking Techniques and Risks

One common prompt hacking technique involves crafting inputs that bypass the model's intended constraints, such as the "grandmother exploit," where attackers manipulate the model into providing disallowed information by framing the request in a specific context.

Attackers may use prompt injection attacks to override system prompts or extract confidential data that the model has been exposed to during training. In applications like chatbots, virtual assistants, or interactive voice response (IVR) systems, attackers with knowledge of the underlying LLM can manipulate prompts to:

- Inject malicious content: Causing the LLM to generate harmful or inappropriate responses that could damage the organization's reputation or lead to legal issues.
- Exfiltrate data: Extracting sensitive information from the model, such as proprietary data or personally identifiable information (PII) that the model has been trained on.
- Manipulate decision-making processes: Influencing the outputs of the LLM in ways that could affect business decisions, customer interactions, or automated systems.



The risks associated with LLM prompt hacking are significant, as successful attacks can compromise data integrity, confidentiality, and system availability. Organizations relying on LLMs for critical functions may face severe consequences, including data breaches, financial losses, and erosion of customer trust.

ANTICIPATED ATTACK 4:
INFLUENCE OF ADVERSARIAL LLMS ENHANCING ATTACK CAPABILITIES

Attackers are increasingly leveraging adversarial Large Language Models (LLMs) to significantly enhance their cyberattack capabilities, posing new challenges to cybersecurity defenses. These malicious LLMs—such as WormGPT, FraudGPT, WolfGPT, and XXXGPT—are designed to generate sophisticated and tailored cyber threats with minimal effort. By utilizing these advanced models, attackers can create highly effective malware, craft convincing phishing emails, and automate the development of exploits.

One of the key concerns is the evasion of traditional security measures. AI-generated malware and exploits can adapt, obfuscate, and mutate to avoid detection by conventional antivirus software and Endpoint Detection and Response (EDR) systems.

The polymorphic nature of AIcrafted code means that signature-based detection methods are less effective, as each iteration can appear unique while maintaining its malicious functionality.

Furthermore, the availability of adversarial LLMs lowers the barrier for novice malicious actors. Individuals with limited technical expertise can now execute complex cyberattacks by simply interacting with these malicious AI models. This democratization of advanced attack capabilities leads to an increase in the volume and sophistication of cyber threats, as more threat actors can launch attacks that previously required specialized skills.

ANTICIPATED ATTACK 5:
QUANTUM COMPUTING - A LOOMING THREAT TO CRYPTOGRAPHY

Quantum computing is set to revolutionize the world of information technology by introducing computational power that vastly exceeds current capabilities. With an exponential increase in processing speed—sometimes described in astronomical terms like 2 to power of 3 to the power of 1000—quantum computers can tackle complex problems that are practically unsolvable by classical computers.

The introduction of quantum computing poses a critical threat to all applications and communication channels that rely on public key infrastructure, digital certificates, and key exchange protocols.

Current encryption methods, both asymmetric algorithms like RSA and symmetric algorithms such as Triple DES (3-DES) and certain key lengths of AES (like 64-bit AES), rely on the computational difficulty of specific mathematical problems. Classical computers find it infeasible to solve these problems within a reasonable timeframe, which is why these encryption methods are considered secure.

However quantum computing holds the potential to break existing encryption algorithms and keys that safeguard our digital communications. Algorithms like Shor's algorithm can factor large numbers and compute discrete logarithms exponentially faster than classical algorithms. This capability effectively renders asymmetric encryption vulnerable. Similarly, Grover's algorithm can speed up the brute-force search process, weakening symmetric encryption by effectively halving the key length.

In such a scenario, we face a situation where the integrity of the sender in any communication cannot be trusted. Intruders equipped with quantum computers could easily break encryption keys and algorithms, enabling them to conduct man-in-the-middle attacks. They could intercept, decrypt, and even alter messages without the sender or receiver being aware, compromising the confidentiality and integrity of the communication.

ANTICIPATED ATTACK 6:
CRYPTO: A NEW FRONTIER FOR CYBER THREATS

Cryptocurrency has significantly altered the cyber threat landscape, empowering intruders in ways that previous technologies could not. Initially, the cyber perpetrators utilized Bitcoin for illicit transactions due to its widespread acceptance. However, they've since migrated to other cryptocurrencies like Monero (XMR), which offer enhanced privacy and non-traceability. Monero's advanced encryption techniques obscure transaction details, making it exceptionally challenging for law enforcement agencies to trace funds and identify the individuals involved.

This shift in cryptocurrency preference has also seen a change in the tactics employed by intruders. They have evolved from using compromised systems merely as crypto miners—where infected computers are hijacked to mine cryptocurrencies without the owner's knowledge—to more direct and profitable endeavours like targeting cryptocurrency exchanges. By attacking these exchanges, intruders aim to steal large amounts of digital currency, exploiting security vulnerabilities within these platforms.

Additionally, a new breed of malware has emerged that goes beyond the traditional goal of harvesting Personally Identifiable Information (PII). These sophisticated malware programs scan infected environments not just for sensitive data but specifically for the presence of cryptocurrency wallets or the keys that secure them. By extracting these keys, intruders can gain unauthorized access to victims' crypto assets, leading to significant financial losses.

The evolution of cryptocurrency has also facilitated the rise of ransom and data extortion schemes. Malicious actors now commonly demand payment in cryptocurrencies, leveraging their anonymity to avoid detection.

This trend has led to the development of an entire ecosystem designed to support these illicit transactions. Services and platforms have emerged to facilitate the exchange, laundering, and obfuscation of cryptocurrency funds, making it easier for intruders to monetize their activities without leaving a traceable trail.

ANTICIPATED ATTACK 7:
IoT, THE EMERGING THREATS TO EMBEDDED DEVICES

Cloud-Connected Embedded Devices

Embedded devices increasingly rely on cloud services like Amazon Elastic Compute Cloud (AWS EC2) and Message Queuing Telemetry Transport (MQTT) brokers to transmit and store data. These devices collect sensor or user data and push it to services like AWS S3 using temporary credentials assigned by the cloud. While efficient, this creates vulnerabilities—compromised credentials from one device can grant attackers access to the larger cloud infrastructure. If thousands of devices share identical configurations, breaching one can expose the entire fleet, risking data theft, lateral movement, or operational disruption.

Firmware Reverse Engineering, IP Theft, Digital Twins & Secret Extraction

Firmware holds the core intellectual property (IP) and operational logic of embedded devices, making it a high-value target for attackers. By reverse engineering firmware, adversaries can inject malicious code, alter device behavior, or create "digital twins" that mimic legitimate devices while feeding manipulated data into real systems. This can disrupt critical operations, especially in environments where devices control physical processes or infrastructure. Additionally, firmware often contains proprietary algorithms and secrets, allowing attackers to clone products, bypass protections, or extract shared encryption keys embedded across entire product lines. A single compromised device can expose an entire fleet, enabling adversaries to escalate privileges, manipulate data, or propagate malware across interconnected systems, threatening IP, operational security, and product integrity.

OTA Updates & Single-Device Pivot

Over the air (OTA) updates simplify firmware patching but introduce significant risk. A compromised update server can distribute malicious firmware, bricking devices or causing widespread failures. Attackers can exploit open debug interfaces to reverse engineer firmware and tamper with the OTA process. Since firmware is often identical across devices, malicious updates propagate rapidly, turning a single breach into a system-wide threat.

Hardware Trojans, chip backdoor & "Movie-Style" Attacks in real life

Hardware Trojans—malicious circuit modifications—can be inserted during chip fabrication or assembly. Attackers or nation-states can implant these rogue components that remain dormant until triggered. An extra chip can be concealed beneath a Ball Grid Array (BGA) package or masked with high-temperature adhesives, making detection nearly impossible without specialized forensics. These implants enable remote takeovers, allowing attackers to control infrastructure with a single command. In large-scale deployments, compromising one node can escalate to entire networks. Lack of PCB-level inspections leaves critical systems vulnerable to these stealthy attacks.

Scalability of Attacks, Mod Chips, Side-Channel Analysis and Glitching

Hardware exploits, once developed, can be mass-produced through mod chips or glitching techniques. Mod chips—initially used to bypass gaming console security—can scale to automotive and IoT systems, bypassing protections at scale. Side-channel analysis reveals sensitive data by monitoring power consumption or electromagnetic leaks, while voltage faults at critical moments can bypass security checks. These scalable methods transform niche vulnerabilities into widespread threats, compromising even highly secure systems.

RECOMMENDATIONS: STRENGTHENING YOUR CYBERSECURITY POSTURE

RECOMMENDATIONS: STRENGTHENING YOUR CYBERSECURITY POSTURE

Having explored the TTPs (Tactics, Techniques, and Procedures) used by attackers, examined unique case studies showcasing their stealth and evasion techniques, and gained a glimpse into the anticipated trends of 2025, it's time to focus on the critical question: What can organizations do to stay secure?

The solution lies in establishing effective, adaptable, and forward-thinking cybersecurity strategies.

The following section highlights the key controls organizations should implement, based on insights from audit and incident analysis findings, to strengthen defenses, mitigate vulnerabilities, and effectively protect sensitive data. These recommendations aim to empower organizations to stay ahead in an ever-evolving threat landscape while enhancing operational efficiency and resilience.

ADAPTABLE, FORWARD-THINKING CYBERSECURITY IS BUILT ON KEY CONTROLS THAT DEFEND, MITIGATE, AND PROTECT.

ENHANCING RESILIENCE ACROSS KEY DOMAINS

PEOPLE

(Awareness, Training, and Culture)

- Increase the Frequency of Information Security Training
- Strengthen Risk Management and Governance
- Focus on Securing Remote and Hybrid Work Technologies

PROCESS

(Policies, Procedures, and Governance)

- Accelerate Vulnerability Assessments Time Frame
- Develop Comprehensive Incident Response Playbooks
- Integrate Threat Intelligence into Monitoring Processes
- Defense-in-depth program
- Zero Trust Architecture (ZTA) Implementation

TECHNOLOGY

(Tools, Systems, and Solutions)

- Increase the Frequency of Patching Network Devices
- Implement AI-Powered Anomaly Detection and Dark Web Monitoring
- Application and API Security
- Authentication and Access Control
- Endpoint and Email Security
- Security Testing of AI-Native Applications

BUILDING A RESILIENT PEOPLE - FORCE: STRENGTHENING CYBERSECURITY THROUGH TRAINING, GOVERNANCE, AND REMOTE SECURITY

A strong and adaptable cybersecurity posture begins with people. Organizations must foster a culture where cybersecurity awareness is continuous, leadership-driven, and embedded across all levels.

Continuous Information Security Training

Transitioning from annual to quarterly security training enhances resilience by keeping employees vigilant against evolving threats like AI-driven phishing and deepfake scams. Frequent education ensures that staff stay informed about emerging attack vectors and reinforces proactive security behavior. By involving the entire workforce, from executives to frontline employees, organizations establish a unified defense against social engineering tactics.

Leadership plays a crucial role in shaping this culture. When executives prioritize cybersecurity and actively champion training initiatives, it signals the importance of security as part of the broader business strategy. This top-down approach not only protects sensitive data but also builds customer trust and solidifies the organization's long-term success.

Securing Remote and Hybrid Work Environments

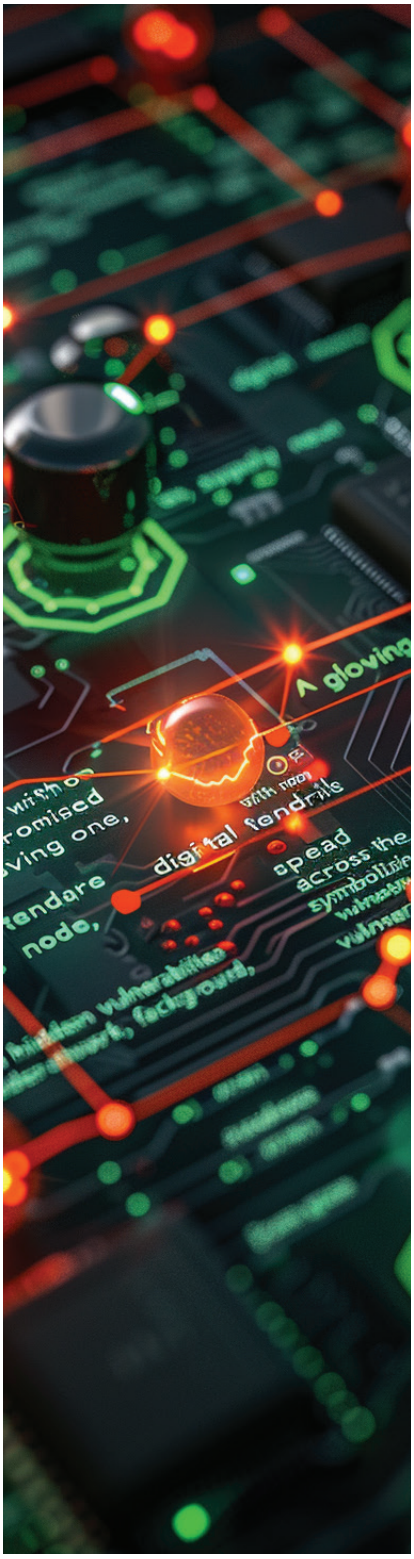
As remote and hybrid work models expand the attack surface, organizations must secure the technologies that support these environments. Conducting regular vulnerability assessments, enforcing timely patching, and strengthening remote access solutions are essential steps. High-profile incidents, such as the MOVEit Transfer vulnerabilities, underscore the critical need for ongoing vigilance in securing internet-facing systems and remote infrastructure.

Risk Management and Governance for Long-Term Resilience

A proactive, comprehensive risk management framework is essential to enhance regulatory adherence and fortify the overall security posture. This framework drives transparency, enables standardized reporting, and facilitates benchmarking against industry best practices. Strong governance mechanisms ensure accountability, incident disclosure, and effective resource allocation to mitigate risks.

Regular security assessments, incident monitoring, and performance tracking through metrics—such as known vulnerabilities and training completion rates—provide actionable insights that drive timely adjustments. Governance structures that evaluate AI-related risks, adversarial threats, and ethical concerns position organizations to address emerging vulnerabilities before they escalate.

By integrating cybersecurity governance into the organization's core, businesses not only enhance regulatory compliance but also foster resilience against increasingly sophisticated threats. This holistic approach ensures that cybersecurity measures align with broader business objectives, empowering the organization to navigate and thrive in a complex digital landscape.



STRENGTHENING CYBERSECURITY THROUGH PROACTIVE PROCESSES AND LAYERED DEFENSES

Effective cybersecurity relies on processes that not only anticipate threats but also build resilience through continuous monitoring, adaptive defense strategies, and structured responses.

By embedding dynamic processes, organizations can minimize vulnerabilities, streamline detection, and respond swiftly to emerging threats.

Accelerated Vulnerability Assessments

In today's rapidly evolving threat landscape, waiting for quarterly or annual vulnerability assessments is no longer sufficient. Conducting daily or weekly assessments using automated solutions is essential to identify and mitigate weaknesses before attackers exploit them. The time between vulnerability disclosure and exploitation has drastically shortened, making real-time scanning a critical component of organizational security. Automated tools ensure systems are continuously monitored, allowing teams to prioritize remediation and close security gaps swiftly.

Threat Intelligence Integration

As adversaries grow more sophisticated, the integration of threat intelligence into monitoring processes is crucial. Threat actors often share tools and vulnerabilities, necessitating collective action and intelligence sharing. Organizations must incorporate reputable threat feeds (such as from CERT-In) into their security frameworks to proactively detect attack patterns. This intelligence-driven approach enables faster response times and anticipates threats based on evolving tactics, strengthening defenses across the board. By fostering collaboration between vendors, enterprises, and industry peers, organizations create a unified defense that mirrors the interconnected strategies used by threat actors.

Defense-in-Depth as a Strategic Imperative

No single solution can fully protect against modern cyber threats. Defense-in-Depth offers a layered strategy where multiple controls—firewalls, intrusion prevention, and endpoint detection—work in tandem to detect, delay, or mitigate attacks. This holistic framework extends beyond technology, incorporating policies and procedures that reinforce organizational resilience. Endpoint Detection and Response (EDR) tools play a pivotal role in addressing AI-driven and customized malware threats, bridging the gap left by traditional antivirus solutions. This layered approach creates redundancies, ensuring that even if one control fails, others remain active to contain breaches.

Comprehensive Incident Response Playbooks

Preparedness is critical. Standardized playbooks for responding to diverse cyber incidents ensure that teams act quickly, uniformly for the type of incident and decisively. These playbooks guide analysis, containment, and mitigation, reducing the chance of oversight during critical moments. By establishing predefined response protocols, organizations can streamline investigations, minimizing operational disruptions and financial losses.

Zero Trust Architecture (ZTA) for Modern Threats

The traditional network perimeter is no longer sufficient as remote work, cloud services, and mobile devices expand the attack surface. Zero Trust Architecture (ZTA) enforces continuous authentication, granular access control, and micro-segmentation to safeguard sensitive assets. By assuming that no user or device can be implicitly trusted, ZTA reduces lateral movement and limits the damage potential of compromised credentials or insider threats.

Proactive processes form the backbone of a resilient cybersecurity strategy. By accelerating assessments, embedding intelligence, deploying layered defenses, and implementing Zero Trust, organizations can build robust frameworks that withstand evolving threats.

TECHNOLOGY: BUILDING RESILIENT CYBER DEFENSES

Accelerate Patching of Network Devices

Network devices are prime targets for attackers, with vulnerabilities in firewalls and VPNs surging by 229% in the past year. Zero-day exploits are being weaponized faster, with some attacks launched within hours of disclosure. To stay ahead, organizations must aggressively patch network devices on a continuous basis, reducing exposure and closing critical gaps before exploitation occurs. This proactive stance is essential to safeguard infrastructure from evolving AI-powered attack techniques.

AI-Driven Anomaly Detection and Dark Web Monitoring

Traditional security tools fall short against stealthy, adaptive threats. AI-powered anomaly detection continuously monitors for irregular behaviors that evade standard defenses. These systems can identify subtle deviations in user behavior, pinpointing malicious activities hidden within normal operations. Simultaneously, dark web monitoring ensures early detection of compromised credentials, allowing organizations to enforce rapid password resets and mitigate potential breaches before they escalate.

Strengthen Authentication and Access Control

Multi-Factor Authentication (MFA) must be enforced across all sensitive financial operations (e.g., NEFT/RTGS). This ensures robust identity verification and mitigates insider threats. Strict access control lists should be maintained and regularly reviewed to prevent overprovisioned accounts. Applying the principle of least privilege reduces unnecessary access, narrowing the attack surface and minimizing potential damage from compromised accounts.

Application and API Security

APIs represent a critical attack vector, especially in AI-native and payments ecosystems. To mitigate threats:

- Secure APIs with strong authentication (OAuth, JWT, API keys) and enforce IP whitelisting.
- Use server-to-server validation to safeguard sensitive transactions, avoiding browser redirects.
- Implement CORS (Cross-Origin Resource Sharing) restrictions to prevent unauthorized domains from accessing APIs.

By locking down API access and restricting sensitive documentation, organizations can reduce risks of API-driven data breaches and unauthorized system interactions.

Endpoint and Email Security

Endpoints remain a primary entry point for phishing and ransomware. Application whitelisting should be enforced to block unauthorized software, while robust email and web filters intercept phishing attempts and malicious advertisements. Keeping antivirus solutions updated and restricting unnecessary remote-access tools further strengthens endpoint defenses. Limiting exposure at this level reduces the likelihood of breaches escalating across the network.

Securing AI-Native Applications

APIs within AI-native applications are often overlooked during development. API security testing must be embedded early in the Software Development Lifecycle (SDLC) to uncover hidden vulnerabilities. By expanding Dynamic Application Security Testing (DAST) to cover API endpoints, organizations address gaps that traditional scanning might miss. Proactive testing against OWASP Top 10 API vulnerabilities ensures AI systems are protected at scale.

Through a layered technological defense, organizations can reduce exploitable weaknesses, safeguard sensitive operations, and stay resilient in the face of rapidly evolving cyber threats.

CONCLUSION

CONCLUSION

And with that, CERT-In, CSIRT-Fin and SISA wrap up this year's journey through the shifting sands of the cybersecurity landscape. We hope this report has provided you with meaningful insights, actionable takeaways, and maybe even a fresh perspective on the challenges we collectively face.

The BFSI industry stands at a unique intersection of opportunity and risk. As non-cash transactions continue to grow at an extraordinary pace, fueled by the shift to e-commerce and the digitization of B2B payments, the sector is transforming into an increasingly complex ecosystem. While these advancements open new doors for innovation and customer engagement, they also present attractive targets for cyber adversaries seeking to exploit vulnerabilities for gain.

The journey to secure this ecosystem is far from over. Threats are constantly evolving, and as technology advances, so do the tactics and motives of those seeking to disrupt it. The digital payments sector, with its immense value and increasing reliance on interconnected systems, requires constant vigilance and adaptability to protect against emerging risks.

We hope this report serves as a valuable resource in helping you identify potential vulnerabilities, prepare for the unexpected, and prioritize investments in your cybersecurity strategies. At the heart of this effort is the shared goal of building a secure digital society—one that safeguards trust, innovation, and growth.

We want to extend our heartfelt thanks to the many contributors who helped bring this report to life, from data partners to researchers, whose expertise and collaboration made it possible. And to you, our readers, thank you for your continued engagement, feedback, and commitment to advancing cybersecurity.

The road ahead will undoubtedly be filled with challenges, but with the right insights, preparation, and dedication, it's a road we can navigate together. Here's to building a safer and more secure future for all.

ACKNOWLEDGEMENTS

We express our deepest gratitude to our customers and partners, whose trust and collaboration are the cornerstone of our efforts. Engaging with them not only helps us exchange knowledge but also drives our continuous growth and learning. Together, we share a vision of building a more secure and resilient digital ecosystem.

A huge thanks to SISA'ites, officers of CSIRT-Fin (Computer Security Incident Response Team for the Indian Financial Sector) and CERT-In (Indian Computer emergency Response Team), whose contributions have been instrumental in the creation of this report. Their ability to synthesize findings, provide insights, and bring this analysis to life underscores the incredible talent, depth and dedication within the respective teams.

This report is a product of collective effort, collaboration, and shared commitment to cybersecurity, and we are immensely grateful to everyone who made it possible.

REFERENCES

1. https://www.ibm.com/reports/data-breach
2. https://www.business-standard.com/finance/news/average-cost-of-data-breaches-in-india-hits-2-18-million-rbi-report-124072900610_1.html
3. https://www.financialexpress.com/life/technology-phishing-attacks-on-financial-sectors-soar-in-india-increasing-by-175-in-2024-report-3669276/
4. SISA Forensics Investigations
5. SISA Forensics Investigations
6. Verizon DBIR 2024: Five Compelling Stats
7. https://cointelegraph.com/news/engineer-hacks-trezor-wallet-recovers-2m-in-lost-crypto
8. https://panaseer.com/resources/reports/2022-security-leaders-peer-report

https://www.sharefile.com/resource/blogs/cybersecurity-trends
https://www.beyondtrust.com/blog/entry/beyondtrust-cybersecurity-trend-predictions
https://blog.shi.com/cybersecurity/are-you-protected-2025s-top-cybersecurity-trends-and-strategies-to-follow-now/
https://medium.com/@DataFlowX/the-future-of-cybersecurity-predictions-and-trends-for-2025-21e95173d1e9
https://www.pwc.com/gx/en/tmt/5g/pwc-securing-5gs-future.pdf
https://www.sharefile.com/resource/blogs/cybersecurity-trends
https://www.beyondtrust.com/blog/entry/beyondtrust-cybersecurity-trend-predictions
https://blog.checkpoint.com/security/2025-cyber-security-predictions-the-rise-of-ai-driven-attacks-quantum-threats-and-social-media-exploitation/
https://www.weforum.org/stories/2024/10/cyber-resilience-emerging-technology-ai-cybersecurity/
https://www.forbes.com/councils/forbestechcouncil/2024/07/11/the-future-of-cybersecurity-emerging-threats-and-how-to-combat-them/
https://blog.checkpoint.com/research/ransomwares-evolving-threat-the-rise-of-ransomhub-decline-of-lockbit-and-the-new-era-of-data-extortion/
https://www.scworld.com/news/north-korean-nation-state-threat-actor-using-play-ransomware
https://www.datacenterknowledge.com/data-storage/evolving-ransomware-threats-why-offline-storage-is-essential-for-modern-data-protection
https://www.scmr.com/article/regulations-are-forcing-organizations-to-address-software-supply-chain-security/procurement
https://cybersecurityventures.com/software-supply-chain-attacks-to-cost-the-world-60-billion-by-2025/
https://www.scmr.com/article/supply-chain-cyberattacks
https://venturebeat.com/security/forresters-ciso-budget-priorities-for-2025-focus-on-api-supply-chain-security/
https://cybersecurity-magazine.com/why-are-supply-chain-attacks-increasing/
https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/supply-chain-attacks-cyber-threat.html
https://fintechmagazine.com/articles/why-the-finance-sector-grapples-with-software-security-debt
https://hbr.org/2024/10/phishing-attacks-are-evolving-heres-how-to-resist-them
https://flashpoint.io/blog/russian-apt-groups-cyber-threats/
https://www.thisdaylive.com/index.php/2024/09/26/top-vulnerabilities-in-iot-devices-what-hackers-target-how-to-defend-against-them/
https://www.zscaler.com/press/zscaler-threatlabz-finds-400-increase-iot-and-ot-malware-attacks-year-over-year-underscoring
https://www.paymentsjournal.com/asia-overtakes-north-america-as-leading-crypto-development-hub/
https://www.statista.com/statistics/1393453/crypto-payments-global-market-size/
https://www.darkreading.com/cyberattacks-data-breaches/cryptocurrency-attacks-quadrupled-cybercriminals-cash-in
https://www.thomsonreuters.com/en-us/posts/government/identity-theft-drivers/
https://venturebeat.com/security/how-ai-driven-identity-attacks-are-defining-the-new-threatscape/
https://www.scworld.com/resource/why-identity-has-become-a-trojan-horse-and-what-to-do-about-it
https://www.techbusinessnews.com.au/blog/ai-driven-cyber attacks-the-alarming-surge/
https://www.londondaily.news/unlocking-the-potential-of-5g-technology-opportunities-and-challenges-ahead/
https://www.techradar.com/pro/the-rise-of-identity-related-cyberattacks-costs-challenges-and-the-role-of-ai
https://www.techmagic.co/blog/ai-in-cybersecurity
https://www.micromindercs.com/blog/ai-threat-intelligence-empowering-cybersecurity
https://securityintelligence.com/articles/3-proven-use-cases-for-ai-preventative-cybersecurity/
https://www.intelligentcio.com/eu/2024/04/22/the-role-of-cybersecurity-in-securing-critical-infrastructure/

REFERENCES

https://www.auditboard.com/blog/security-vs-compliance/
https://www.tripwire.com/state-of-security/compliance-vs-security-striking-right-balance-cybersecurity
https://www.scrut.io/post/how-to-prevent-cyberattacks-by-balancing-security-and-compliance
https://www.securitymagazine.com/articles/99259-compliance-and-security-are-two-sides-of-the-same-coin
https://www.tripwire.com/resources/guides/mind-the-cybersecurity-compliance-gap
https://www.csoonline.com/article/1309993/grc-impact-and-challenges-to-cybersecurity.html
https://www.mckinsey.com/industries/financial-services/our-insights/global-payments-in-2024-simpler-interfaces-complex-reality
https://cxotoday.com/interviews/turning-data-breaches-into-opportunities-strategies-for-indian-businesses-to-strengthen-cybersecurity-and-reduce-risks/
https://www.scworld.com/resource/building-cybersecurity-resilience-strategies-technologies-and-best-practices-from-industry-leaders
https://www.techtarget.com/searchsecurity/tip/5-tips-for-building-a-cybersecurity-culture-at-your-company
https://www.weforum.org/stories/2024/04/cybersecurity-key-strategies-cyber-resilience-2024/
https://www.techtarget.com/searchsecurity/feature/Security-posture-management-a-huge-challenge-for-IT-pros
https://www.techtarget.com/healthtechsecurity/feature/Navigating-cyber-insurance-coverage-as-threats-evolve
https://www.helpnetsecurity.com/2024/07/05/iot-security-privacy-challenges/
https://www.paloaltonetworks.com/cybersecurity-perspectives/how-to-secure-iot-in-financial-services
https://securityintelligence.com/articles/what-are-the-risks-of-the-iot-in-financial-services/
https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

SISA

SISA is a forensics-driven cybersecurity company solutions provider specializing in securing the digital payments industry. As a Global Payment Forensic Investigator of the PCI Security Standards Council, we leverage forensics insights into preventive, detective, and corrective security solutions, protecting 1,000+ organizations across 40+ countries from evolving cyberthreats. Our suite of solutions from AI-driven compliance, advanced security testing, agentic detection/ response and learner focused-training has been honored with prestigious awards, including from Financial Express, DSCI-NASSCOM and The Economic Times. With commitment to innovation, and pioneering advancements in Quantum Security, Hardware Security, and Cybersecurity for AI, SISA is shaping the future of cybersecurity through cutting-edge forensics research.

CERT-In

CERT-In is the national agency for responding to computer security incidents as and when they occur. In the Information Technology Amendment Act 2008,CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection,analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents.
- Emergency measures for handling cyber security incidents.
- Coordination of cyber incident response activities.
- Issue guidelines,advisories,vulnerability notes and whitepapers relating to information security practices,procedures, prevention,response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed
  Refer www.cert-in.org.in for more details

CSIRT-Fin

Computer Security Incident Response Team in Finance sector (CSIRT-Fin) , is a nodal sectoral CSIRT which provides Incident Prevention and Response services as well as Security Quality Management Services to the entities of the Indian financial sector. It manages cyber incidents and coordinate responses across banking, securities market infrastructure, insurance, and pension funds entities.

It carries out the following roles related to the cyber security in financial sector:

i. Collection, analysis & dissemination of information on cyber incidents.
ii. Forecast and alerts on cyber security incidents.
iii. Emergency measures on cyber security incidents.
iv. Coordination for cyber incident response activities.
v. Issue guidelines, advisories, vulnerability, and white papers relating to information security.
vi. Monitor sectoral efforts in the financial sector towards maintaining dynamic and modern cyber security architecture, developing awareness amongst regulated entities and public in general.
vii. Such other functions relating to cyber security in the financial sector, as may be prescribed.