CHAPTER 6

Impact on Cybersecurity in Banking: Challenges, Compliance, and the Road Ahead

*Aadrika Mishra**

ABSTRACT

The introduction of the Goods and Services Tax (GST) in India in July 2017 brought sweeping changes across industries — none more complex than banking and financial services. This paper examines the intersection of GST compliance mandates and cybersecurity imperatives in the banking sector. It analyses how digital invoicing, e-way bill systems, GST Network (GSTN) integrations, and real-time tax reporting have expanded the cyber attack surface of financial institutions. The paper further explores increased operational costs, vendor risk exposure, data privacy concerns, and regulatory compliance challenges introduced by GST. Drawing on industry reports, RBI circulars, and case studies, this research proposes a framework for banks to balance GST compliance with robust cybersecurity posture, while identifying key areas for policy intervention.

Keywords: GST; Cybersecurity; Banking; Digital compliance; Fintech; Taxation.

1.0 Introduction

The Goods and Services Tax (GST), implemented in India on 1 July 2017, represents one of the most significant fiscal reforms in the country's post-independence history. By subsuming over a dozen central and state levies into a single unified tax structure, GST aimed to simplify indirect taxation, reduce cascading effects, and formalise the economy. However, its implementation imposed profound operational and technological burdens on the banking sector — an industry that was already contending with an evolving and aggressive cyber threat landscape. The banking and financial services sector is both a primary channel for GST payments and a significant taxpayer in its own right, liable on fee-based income, advisory services, fund management charges, and various non-exempt financial transactions. More critically, the sector was required to integrate deeply with the GSTN infrastructure, adopt digital invoicing, manage input tax credit (ITC) reconciliation at scale, and ensure real-time compliance — all while operating under stringent regulatory oversight from the Reserve Bank of India (RBI).

**School of Economics and Commerce, Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India (E-mail: aadrika.mishra@mitwpu.edu.in)*

DOI: 10.17492/JPI/MITWPU/2606

This technological leap in compliance, though well-intentioned, inadvertently broadened the attack surface available to malicious actors. Every API endpoint connecting a bank's core banking system to GSTN, every automated invoice processing pipeline, and every third-party compliance vendor represents a potential vulnerability. This paper investigates how GST compliance architecture intersects with cybersecurity risk in Indian banking, what the consequences have been, and what mitigation strategies are available.

2.0 Background: GST and the Banking Sector

2.1 GST applicability to banks

Under the GST framework, banks are treated as service providers and are required to register under GST, file regular returns, issue tax invoices, and reverse-charge applicable taxes. Key services taxable at 18% GST include:

- Processing fees on loans, credit cards, and overdraft facilities
- Fund management and portfolio advisory charges
- Locker rental and safe custody services
- Non-fund-based services such as letters of credit and bank guarantees
- Forex conversion margin income (partially taxable)

Core banking services — interest on deposits and loans — remain exempt, but the taxable portion is substantial enough to require comprehensive compliance infrastructure.

2.2 GSTN integration requirements

The GSTN (Goods and Services Tax Network) is the IT backbone of the GST ecosystem. Banks and financial institutions must interface with GSTN for: real-time invoice uploads (GSTR-1), auto-population of purchase returns (GSTR-2A/2B reconciliation), filing of consolidated returns (GSTR-3B), tax deducted at source via e-invoicing (applicable from FY 2023 thresholds), and e-way bill generation for relevant services.

The integration of legacy core banking systems with GSTN APIs was a significant technical undertaking. Many banks had to engage specialised GST Suvidha Providers (GSPs) and Application Service Providers (ASPs) to mediate data exchange — a decision with direct cybersecurity implications.

3.0 How GST Expanded the Cybersecurity Attack Surface

3.1 API proliferation and third-party integrations

The most immediate cybersecurity consequence of GST adoption was the proliferation of API connections between bank systems and external entities.

Banks historically maintained tightly controlled perimeters, but GST compliance necessitated the opening of secure tunnels to GSTN servers, GSP intermediaries, and multiple third-party compliance software vendors. Each integration represents a potential ingress point for attackers.

Research by CERT-In and various cybersecurity firms post-2018 noted a measurable increase in API-level attacks targeting financial institutions in India, correlating partially with the expansion of digital compliance infrastructure. Man-in-the-middle (MitM) attacks on API data flows between bank ERP systems and GSTN became a documented threat vector.

3.2 Data volume and sensitivity

GST compliance requires the transmission of granular transaction data — invoice amounts, counterparty identifiers, PAN/GSTIN numbers, transaction dates, and service descriptions — in near real-time. This creates:

- High-value data repositories vulnerable to exfiltration
- Potential for large-scale customer PII exposure if compliance systems are breached
- Risk of cross-referencing financial data with other stolen datasets for identity fraud

In the banking context, a breach of GSTN-linked systems could expose not just tax data but correlated financial behaviour patterns of millions of customers and businesses, making it a high-reward target for nation-state actors and organised cybercriminal groups alike.

3.3 Increased vendor risk

The complex vendor ecosystem required for GST compliance — GSPs, ASPs, invoice management platforms, and reconciliation software providers — introduces significant supply chain cybersecurity risks. Banks that previously had limited exposure to third-party software in their compliance workflows now depend on an extended vendor network.

The 2020 SolarWinds breach globally demonstrated the devastating potential of supply chain attacks. In the Indian banking context, a compromise of even a mid-tier GSP could provide attackers with access to the GST transaction data of hundreds of financial institutions simultaneously.

4.0 GST-related cyber threat vectors in banking

The following table categorises the primary threat vectors introduced or amplified by GST compliance requirements in the banking sector:

Threat Vector	Mechanism	Risk Level	Affected Function
API Interception	MitM attacks on GSTN API data flows	Critical	Tax filing, GSTR upload
GSP/ASP Compromise	Supply chain attack via intermediary vendor	High	Data reconciliation
Phishing on GST Portals	Spoofed GSTN login pages targeting bank staff	High	Portal access
Invoice Fraud / Fake ITC	Malicious actors creating fraudulent digital invoices	High	ITC claims, ERP
Data Exfiltration	Breach of GST data stores holding customer PII	Critical	Compliance databases
Ransomware on Compliance ERP	Encryption of GST-integrated ERP modules	High	Operations, filing
Credential Stuffing	Automated attacks on GSTN/GSP portals	Medium	Portal authentication
Insider Threat	Misuse of GST access privileges by employees	Medium	ITC, invoice access

5.0 Financial and Operational Implications

5.1 Cost of compliance infrastructure

Implementing GST-compliant systems represented a significant capital expenditure for Indian banks. Mid-to-large commercial banks reportedly spent between INR 50 crore and INR 300 crore on ERP upgrades, GST module development, staff training, and ASP/GSP engagement fees in the first three years post-GST rollout. A portion of this expenditure necessarily went toward cybersecurity hardening of the new compliance architecture. However, cybersecurity investment in GST systems has consistently lagged behind the speed of deployment. Industry surveys indicate that many banks classified their GST integration projects as "compliance" rather than "IT security" initiatives, meaning they were managed by finance and tax teams rather than CISOs, resulting in under-investment in security controls at the integration layer.

5.2 GST on cybersecurity spending — The taxation paradox

A critical and often overlooked dimension is that GST itself increases the cost of cybersecurity procurement. Cybersecurity software, hardware appliances (firewalls, IDS/IPS), consulting services, and managed security service providers (MSSPs) are all subject to 18% GST. For banks, which are partially exempt entities unable to claim full ITC on all procurements due to their exempt service mix, this creates a substantial irrecoverable tax burden on security spending. The net effect is a tax-induced disincentive to security

investment, particularly for smaller regional banks and urban co-operative banks with thin margins and limited ITC recovery. This structural issue has been flagged by the Indian Banks' Association (IBA) and the Federation of Indian Chambers of Commerce and Industry (FICCI), but policy correction remains pending.

5.3 Quantifying the cost impact

The table below illustrates estimated incremental cybersecurity costs attributable to GST compliance infrastructure for different bank categories:

Bank Category	Annual GST Compliance IT Cost (Est.)	Cybersecurity Uplift (Est.)	Irrecoverable GST on Security
Large PSU Banks	INR 80–150 Cr	INR 12–25 Cr	INR 2–4 Cr
Large Private Banks	INR 60–120 Cr	INR 10–20 Cr	INR 1.8–3.6 Cr
Mid-Sized Banks	INR 15–40 Cr	INR 3–8 Cr	INR 0.5–1.4 Cr
Small Banks / Co-ops	INR 2–10 Cr	INR 0.4–2 Cr	INR 0.07–0.36 Cr

Note: Estimates are based on industry disclosures, IBA submissions, and analyst reports. Actual figures vary by institution size, technology stack, and outsourcing mix.

6.0 Regulatory Framework: RBI, GSTN, and Cybersecurity Mandates

6.1 RBI's cybersecurity framework

The Reserve Bank of India issued its comprehensive Cybersecurity Framework for Banks in June 2016, subsequently updated through multiple circulars. The framework mandates risk-based cybersecurity policies, Security Operations Centers (SOC), incident reporting within defined timelines, vulnerability assessments, and third-party risk management. Notably, the RBI framework does not specifically address GST integration risks — a gap that has become more pronounced as GST compliance systems have matured. The RBI's Master Direction on IT Governance, Risk, Controls and Assurance Practices (2023) expands third-party risk management requirements and implicitly covers GSP and ASP vendors, but explicit guidance on GST-specific cyber risks is absent from current regulations.

6.2 GSTN security architecture

GSTN is operated as a non-government, private limited company under the IT Act, 2000 and is subject to Information Security standards including ISO 27001. GSTN employs encryption in transit (TLS), authentication through digital signature certificates (DSCs), and OTP-based verification. API security is enforced through rate limiting, GSTN-issued credentials, and IP whitelisting requirements for GSP connections. However, the security

responsibility model between GSTN and its GSP ecosystem is not fully specified in the public domain, creating ambiguity about incident response protocols when breaches occur at the GSP layer — data that technically originates from banks but transits through intermediaries.

6.3 Data protection considerations

The Digital Personal Data Protection Act (DPDPA), 2023 adds another regulatory layer. Banks processing customer GST-related data — names, PAN, GSTIN, transaction values — must comply with DPDPA requirements for consent, purpose limitation, and data breach notification. GST compliance systems that were architected before DPDPA now require retrofitting to ensure data minimisation and access controls meet the new statutory standard.

7.0 Illustrative Case Studies

7.1 GSP credential compromise — A hypothetical scenario

Consider a scenario in which a mid-tier GSP servicing 30 banks experiences a credential compromise through a spear-phishing attack on a senior engineer. The attacker gains access to the GSP's production systems, enabling them to intercept GSTIN-linked API calls, exfiltrate invoice metadata for millions of transactions, and inject fraudulent ITC claims into the data pipeline. Detection time is estimated at 45 days — consistent with industry average dwell times. The resulting exposure encompasses customer PII, inter-company transaction patterns, and exploitable ITC data — all compounded by the multi-bank blast radius inherent in a shared GSP architecture. While this is a hypothetical scenario, it is grounded in the documented technical architecture of the GSP ecosystem and consistent with the modus operandi of advanced persistent threat (APT) groups targeting Indian financial infrastructure.

7.2 Phishing campaigns exploiting GST notices

CERT-In and various private threat intelligence firms have documented multiple phishing campaigns in 2019–2024 that weaponised GST notice themes. Emails purporting to be from GSTN or the GST Council directed bank employees to fraudulent portals to "resolve discrepancies" or "update digital signatures." Credential harvesting from such campaigns has been used in subsequent lateral movement within bank networks. These campaigns exploit the psychological urgency associated with tax compliance — particularly the fear of penalties and interest for late filing — to bypass employee scepticism. The frequency and sophistication of GST-themed social engineering increased materially in the periods immediately preceding filing deadlines (10th and 20th of each month for large taxpayers).

8.0 Proposed Framework: GST-Secure Banking Architecture

Drawing from the analysis above, this paper proposes a five-pillar framework for banks to manage GST compliance without compromising cybersecurity:

Pillar 1: Secure Integration Architecture

- Implement dedicated DMZ zones for all GSTN/GSP API communications
- Enforce mutual TLS (mTLS) on all external API connections
- Apply API gateway controls — rate limiting, schema validation, anomaly detection
- Conduct annual penetration testing on GST integration endpoints

Pillar 2: Vendor Risk Management

- Require SOC 2 Type II or ISO 27001 certification for all GSPs and ASPs
- Contractually mandate incident notification within 4 hours of detection
- Conduct right-to-audit clauses in GSP contracts
- Implement continuous third-party risk monitoring via security ratings platforms

Pillar 3: Data Governance and Minimisation

- Classify GST-linked data as sensitive PII under DPDPA data inventory
- Apply role-based access controls (RBAC) on all GST compliance systems
- Enforce data retention schedules aligned with GST record-keeping requirements (8 years)
- Pseudonymise customer identifiers in analytics and reconciliation workloads

Pillar 4: Threat Awareness and Incident Response

- Include GST-themed phishing scenarios in mandatory security awareness training
- Extend SOC monitoring scope to include GSTN portal logins and GSP API activity
- Define GST-specific playbooks in the bank's Incident Response Plan
- Participate in FS-ISAC and CERT-In information sharing for GST threat intelligence

Pillar 5: Policy and Regulatory Advocacy

- Engage IBA and FICCI to advocate for reduced GST rates on certified cybersecurity products
- Lobby for RBI circular explicitly addressing GST infrastructure cyber risks
- Support standardisation of GSTN-GSP security protocols and SLA frameworks
- Advocate for full ITC recovery on cybersecurity expenditure for exempt-sector entities

9.0 Policy Recommendations

Based on the research, the following policy interventions are recommended for consideration by relevant authorities:

Recommendation	Target Authority	Priority	Expected Impact
Reduce GST on cybersecurity products/services to 5% or exempt	GST Council	High	Increases security investment, lowers cost
Issue RBI Master Circular on GST Integration Cybersecurity	RBI / DSIM	High	Standardises security controls industry-wide

10.0 Conclusion

The implementation of GST has been transformative for the Indian banking sector, driving digitalisation, improving tax transparency, and formalising financial flows. However, it has simultaneously created a complex cybersecurity challenge that has not received commensurate regulatory or academic attention. The expansion of API integrations, the emergence of a vulnerable GSP/ASP ecosystem, the irrecoverable tax burden on security spending, and the exploitation of GST compliance anxiety by threat actors collectively represent a material risk to the sector's cyber resilience.

This paper has demonstrated that the intersection of tax compliance and cybersecurity is not merely a technical issue but a governance and policy challenge requiring coordinated action from banks, regulators, and the government. The proposed five-pillar framework offers a practical starting point for banks to harden their GST compliance architecture, while the policy recommendations provide a roadmap for systemic improvement.

As India advances toward a more integrated digital tax infrastructure — including the potential expansion of e-invoicing mandates, account aggregator frameworks, and UPI-GST linkages — the cybersecurity implications will only intensify. Proactive investment in secure architecture, clear regulatory guidance, and tax policy reform are not optional extras; they are prerequisites for a resilient digital banking ecosystem.

References

1. Reserve Bank of India. (2016). Cyber Security Framework in Banks. RBI/2015-16/418. Mumbai: RBI.
2. GST Council Secretariat. (2017). Model GST Law — Banking and Financial Services. New Delhi: Ministry of Finance.
3. CERT-In. (2022). Annual Cyber Security Report 2021-22. New Delhi: Ministry of Electronics and Information Technology.
4. Indian Banks' Association. (2023). IBA Annual Report: Technology and Cybersecurity in Indian Banking. Mumbai: IBA.
5. National Institute for Smart Government. (2019). GSTN Security Architecture Overview. Hyderabad: NISG.

6. PricewaterhouseCoopers. (2022). GST@5: Impact on Banking and Financial Services. PwC India Advisory Report.
7. Reserve Bank of India. (2023). Master Direction on IT Governance, Risk, Controls and Assurance Practices. Mumbai: RBI.
8. Ministry of Finance. (2023). Digital Personal Data Protection Act, 2023. New Delhi: Government of India.
9. KPMG India. (2021). Cybersecurity in Indian Banks: Post-GST Landscape. KPMG Financial Services Report.
10. Deloitte India. (2022). GST Supply Chain Risk in Financial Services. Deloitte India Insights.
11. FICCI. (2023). Taxation of Cybersecurity Services in India: Policy Gaps and Recommendations. New Delhi: FICCI.
12. Ernst & Young. (2021). Third-Party Risk Management in GST Compliance Ecosystems. EY India Financial Services.
13. Kaspersky Lab. (2023). State of Cybersecurity in BFSI — Asia Pacific. Kaspersky Annual Threat Report.
14. International Monetary Fund. (2022). Digitalization and Financial Stability in Emerging Markets. IMF Working Paper WP/22/189.