
CYBERSECURITY CHALLENGES FOR WEALTH MANAGEMENT FIRMS IN INDIA

Navigating Digital Threats in India's
Growing WealthTech Landscape



THE CYBERSECURITY LANDSCAPE: A BRIEF INTRODUCTION



OVERVIEW



87% of Indian organizations planning to increase cybersecurity spending in 2025



25% of Indian firms reporting significant cyber losses



Wealth management sector faces unique challenges due to:

- High-value financial data
- Regulatory compliance requirements
- Growing digital transformation
- Increasing sophistication of threats

KEY CYBERSECURITY THREATS

AI-DRIVEN CYBERATTACKS



Sophisticated AI-powered phishing campaigns



Automated exploitation of vulnerabilities



AI used to bypass traditional security measures

RANSOMWARE ATTACKS



Critical threat to data-intensive wealth management systems



Attackers encrypt sensitive client data and demand payment



Growing frequency and sophistication

ADDITIONAL CRITICAL THREATS

THIRD-PARTY & SUPPLY CHAIN BREACHES



Vulnerabilities in vendor and service provider systems



Cybercriminals exploit third-party access to sensitive data



Critical risk in interconnected financial ecosystems

MOBILE SECURITY THREATS



Mobile malware and banking trojans



SIM swapping and account takeover attacks



Unauthorized access to mobile wealth management apps

EMAIL DATA LEAKAGE: THE CRITICAL CHALLENGE

THE PORTFOLIO SHARING DILEMMA

- Wealth management firms routinely share sensitive portfolio details via email with:
 - Clients for portfolio reviews and updates
 - Accountants and tax advisors for tax calculation and filing
 - Third-party financial consultants for planning
- 3.4 billion spam emails sent daily, with many bypassing filters

KEY DATA LEAKAGE RISKS

- Email interception: Unencrypted emails expose client portfolios during transit
 - Wrong recipient: Simple typos can send sensitive data to unauthorized parties
 - Hacked email accounts: 183M email credentials compromised in recent breaches
 - Email forwarding chains: Loss of control once data enters client/accountant inbox
 - Third-party exposure: Accountants' systems may have weaker security controls
-

THE TAX SEASON MULTIPLIER EFFECT

- During tax filing, portfolio data shared with multiple accountants and tax preparers
 - Data often stored on accountant servers with varying security standards
 - IRC Section 7216 violations: Unauthorized disclosure of tax return information
 - Cross-border risks: Offshore tax preparation increases data exposure points
-

SECURE ALTERNATIVES TO EMAIL FOR DATA SHARING

TECHNOLOGY SOLUTIONS

- End-to-end encrypted email services (Mailfence, Tuta, ProtonMail)
- Secure file sharing platforms with encryption:
 - TitanFile, SecureDocs for financial documents
 - Virtual Data Rooms (VDRs) for sensitive portfolio data
- API-based secure connections (replacing email workflows)
 - Direct system-to-system encrypted data transfer
 - Granular access controls and audit logs
- Data Loss Prevention (DLP) solutions with ML-powered monitoring
- Automated encryption for all outbound financial communications

BEST PRACTICES FOR PORTFOLIO SHARING

- Client portals: Secure login-protected dashboards for portfolio access
- Time-limited access links: Auto-expiring secure document links
- Multi-factor authentication (MFA) for all external data sharing
- Granular permissions: Separate access levels for clients vs accountants
- Watermarking and download restrictions on sensitive documents

REGULATORY & COMPLIANCE CHALLENGES

DIGITAL PERSONAL DATA PROTECTION (DPDP) ACT, 2023

- Notified on November 14, 2025
- Requires consent-driven, security-focused approach
- 72-hour breach notification to Data Protection Board
- Mandatory encryption, access controls, and monitoring

RBI DATA LOCALIZATION REQUIREMENTS

- Payment system data must be stored in India
- Foreign processing allowed under strict conditions
- Critical for wealth management payment systems

ORGANIZATIONAL CHALLENGES

CYBERSECURITY SKILL GAP



Shortage of skilled
cybersecurity professionals



60% cite limited expertise in
AI-based cyber defense



50% flag insufficient skills as
primary obstacle

RESOURCE CONSTRAINTS



Limited budgets for comprehensive security programs



Challenge of balancing security with business growth



Need for continuous investment in emerging technologies

STRATEGIC SOLUTIONS & BEST PRACTICES



TECHNOLOGY INVESTMENTS(PRIORITY AREAS)

- AI and Machine Learning for threat detection (61% prioritizing)
- Security tool consolidation (51%)
- Automation solutions (49%)
- Zero Trust architecture implementation

WORKFORCE DEVELOPMENT

- Upskilling and reskilling programs (49% investing)
- Hire specialized cybersecurity professionals
- Focus on AI-based cyber defense expertise

KEY TAKEAWAYS & NEXT STEPS

CRITICAL IMPERATIVES

- Cybersecurity is a business-critical priority, not just IT issue
 - Regulatory compliance (DPDP Act) is mandatory
 - Proactive defense is more cost-effective than reactive response
 - Talent development is as important as technology investment
-

SUCCESS FACTORS

- C-suite commitment and leadership
 - Continuous monitoring and adaptation
 - Collaboration with industry peers and regulators
 - Balance between security and customer experience
-

IMPLEMENTATION ROADMAP

IMMEDIATE ACTIONS(0-3 MONTHS)



Conduct comprehensive
security assessment



Implement mandatory
encryption and access
controls



Establish incident
response protocols



Begin DPDP Act
compliance
documentation

SHORT TERM INITIATIVES(3-12 MONTHS)



Deploy AI-powered
threat detection systems



Launch employee
training programs



Conduct data protection
impact assessments



Strengthen third-party
vendor security



THANK YOU

Vedant Divakarla

CITATIONS

- BreachAlarm. "Email Data Breaches and Compromised Accounts Report." *BreachAlarm*, 2024, www.breachalarm.com.
- Forrester Research. "Zero Trust Architecture Explained." *Forrester*, 2024, www.forrester.com.
- Government of India. *Digital Personal Data Protection Act, 2025*. Ministry of Electronics and Information Technology, 2025, www.meity.gov.in.
- IBM Security. *Cost of a Data Breach Report 2024*. IBM, 2024, www.ibm.com/security/data-breach.
- Microsoft Security. "The Role of AI in Modern Cybersecurity." *Microsoft*, 2024, www.microsoft.com/security.
- Proton AG. "End-to-End Encryption Explained." *Proton*, www.proton.me.
- PwC India. *Global Digital Trust Insights Survey 2024 - India Highlights*. PwC, 2024, www.pwc.in.
- Reserve Bank of India. "Storage of Payment System Data." *RBI Notifications*, 2018, www.rbi.org.in.
- Statista Research Department. "Cyber Crime Losses Reported by Businesses in India." *Statista*, 2024, www.statista.com.
- Statista Research Department. "Number of Spam Emails Sent Per Day Worldwide." *Statista*, 2024, www.statista.com.
- Tutanota GmbH. "Why Encrypted Email Matters." *Tuta*, www.tuta.com.
- World Economic Forum. *Global Cybersecurity Outlook 2024*. WEF, 2024, www.weforum.org.