Cybercrime surge drives rush for white-collar crime lawyers

livemint.com/industry/cybercrime-fraud-ai-rush-for-white-collar-crime-lawyers-11793521108767.html

Krishna Yadav, Yash Tiwari November 2, 2026



India's Digital Personal Data Protection (DPDP) Act, 2023, and DPDP Rules, 2025, set out requirements for consent, data security, breach reporting and individuals' privacy rights**(HT_PRINT)**

Their work is also shifting from routine compliance audits to risk assessment, incident response and investigations, they said. White-collar crimes are typically committed by entities
Cyber fraud is becoming a bigger and more complex threat for India Inc., with criminals impersonating company bosses, siphoning off funds and stealing customer data, sometimes through vulnerable vendors. Now, with artificial intelligence (AI)-enabled scams adding to the risks, white-collar crime teams at law firms are seeing a 20-30% rise in cybersecurity-related advisory and investigation work, lawyers said.

Their work is also shifting from routine compliance audits to risk assessment, incident response and investigations, they said. White-collar crimes are typically committed by entities.

"We have seen a significant increase, perhaps 20-30% more than previous years, in advisory work relating to criminal investigations being conducted by law enforcement agencies into various cybercrimes against or involving technology and banking companies," said Dheeraj Nair, partner at JSA Advocates & Solicitors.

Nair said JSA was advising clients on frozen bank accounts in cyberfraud cases, customer-data theft, police requests for overseas-held data, regulatory reporting and data breach disputes. Companies were also seeking proactive data protection advice.

Shahana Chatterji, partner at Shardul Amarchand Mangaldas & Co., attributed the development to higher regulatory scrutiny. “We have seen a tangible increase in client questions around cybersecurity incidents, specifically on how to effectively manage and mitigate them. This is largely driven by heightened regulatory scrutiny and upcoming obligations under new privacy laws,” said.

India’s Digital Personal Data Protection (DPDP) Act, 2023, and DPDP Rules, 2025, set out requirements for consent, data security, breach reporting and individuals’ privacy rights. With most substantive obligations taking effect on 13 May 2027, companies are reviewing data practices, vendor arrangements and breach-response plans to prepare for compliance.

Supratim Chakraborty, partner at Khaitan & Co., said mandates now covered the entire incident lifecycle, from pre-incident preparedness and legal assistance during attacks to regulatory notifications, communication with affected individuals and post-incident remediation.

The growing legal workload comes as companies ramp up cybersecurity spending. US technology research firm Gartner projected India's information-security spending at $3.4 billion in 2026, up 11.7% from 2025. A Tata Tele Business Services-CMR survey of 800 small and medium enterprise IT heads across eight cities found that 84% planned to increase cybersecurity budgets over the following 12-24 months.

Narasimhan Elangovan, co-founder and cyber security and data privacy practice leader at Ascentium India, said companies were investing in cybersecurity tools and talent to protect assets and build customer trust, with attacks often prompting further spending.

“After an attack, organizations learn a lot through forensics. This leads to incremental investments... Often, incidents are also wake-up calls for many organizations,” he said. Elangovan said companies seek advice on incident response, regulatory reporting, vendor breaches, cyber insurance, compliance of The Digital Personal Data Protection Act, 2023 (DPDP Act), and risks associated with employees using public AI tools.

The changing nature of cyber fraud is reflected in cases law firms are handling.

Kunal Gupta, partner in Trilegal's white-collar crime practice, said fraudsters were using publicly available information, including LinkedIn profiles and regulatory filings, to map corporate hierarchies and impersonate executives through spoofed WhatsApp profiles and emails.

In one case, funds were misappropriated using a spoofed executive identity created through a publicly available domain service. “Such frauds do not always involve technically sophisticated methods. A failure to notice anomalies in an email address or question an unusual payment request can allow relatively simple frauds to succeed,” Gupta said.

JSA has handled cases involving theft of customer information, including credit card and know-your-customer data, through vendors and sub-vendors such as call centres working for banks. “Breaches are taking place not within the client directly, but with a vendor or sub-vendor, who is a weak link,”

Nair said. The firm has also seen fraudsters exploit e-commerce software glitches to obtain both products and refunds, or manipulate electronic gift vouchers.

Khaitan has flagged AI-enabled threats such as phishing, deepfake impersonation of executives and fraudulent payment authorizations. Companies are also concerned about employees inadvertently disclosing confidential information through generative AI tools.

Frauds of all shades

Recent incidents underline these risks.

On 21 October, the country's largest lender State Bank of India disclosed a suspected data leak after identifying 3,897 customer records with personal identifiable information among approximately 3.75 lakh records examined on the dark web.

Two Mumbai-based non-bank lenders reportedly lost around $2 million in more than 700 unauthorized transfers on 8-9 October, according to a *Reuters* report of 30 October. Hackers allegedly compromised the application programming interface (API) used to send loan-disbursement instructions to ICICI Bank.

Tata Electronics had also confirmed a cybersecurity incident in June after a ransomware group claimed to have leaked company data, including documents purportedly linked to Apple and Tesla.

To safeguard against cyberattacks, experts advise companies to conduct regular security audits, assess vendor risks, train employees, enforce multi-factor authentication and maintain tested backups. They also recommend incident-response plans, stronger vendor contracts and clear reporting procedures. In the event of a breach, companies should preserve digital evidence, assess reporting obligations, notify relevant authorities and affected individuals, and inform insurers.

“Thorough due diligence, supply-chain risk management, regular security audits and third-party certifications are essential to limiting the impact of cyber incidents,” said Chatterji from Shardul Amarchand Mangaldas & Co.

Team beef-up

With the number of queries to the law firms soaring, their team sizes have also been ramped up to manage the work.

According to JSA, the firm now has a dedicated team for fintech, data protection and white-collar crimes with the strength of over 70 attorneys. While Trilegal has 13 partners in their white-collar practice and seven partners in technology, media & telecommunications handling these disputes.

Government data highlights the scale of the threat. According to a home ministry press release of 21 July 2026, citing National Crime Records Bureau data, registered cybercrime cases more than doubled to 1,01,928 in 2024 from 50,035 in 2020.

The release also reported over 65.89 lakh financial cyberfraud complaints, involving ₹55,050 crore between 2021 and 2025. The Citizen Financial Cyber Fraud Reporting and Management System had helped save over ₹11,158 crore across over 32.8 lakh complaints as of 30 June, it added.