



CA. Peeyush Sharma

Member of the Institute

Securing the Trust Quotient: A Cybersecurity & Data Protection Framework for Modern CA Practices

Cybersecurity has emerged as a critical practice-management and governance imperative for Chartered Accountants, especially in small and mid-sized firms managing sensitive financial and personal data amid weaker controls. Digitisation, cloud adoption, and remote work have spoiled traditional perimeters, exposing firms to phishing, ransomware,

credential theft, and breaches via insiders or vendors. The article connects these risks to ICAI's confidentiality and due-care duties under the Code of Ethics, IT Act's "reasonable security practices", and the Digital Personal Data Protection Act, 2023 (DPDP Act), with Rules notified in November 2025. It emphasises governance and risk management over mere compliance, while positioning cyber-insurance as a supplementary safeguard rather than a primary control. It describes how digitisation, cloud platforms, and remote work have dissolved the traditional "office boundary", making every user identity and endpoint a potential entry point for cybercriminals using phishing, ransomware, social engineering, silent credential theft, and insider or vendor-driven breaches.

Introduction: From IT Issue to Practice-Risk

Over the last decade, most CA firms have quietly but fundamentally changed how they work. Client interactions that once involved physical files, manual ledgers, and in-person meetings are now dominated by cloud-based accounting systems, online filing portals, shared drives, and video calls. Income-tax returns, GST filings, audit documentation, board packs, and management reports all move through digital channels, often accessed from multiple locations and devices.

This article argues that cyber risk must be treated as an integral part of practice management and professional governance. It maps why CA firms are attractive targets, explains how attacks typically unfold in real life, connects cybersecurity to professional and legal obligations, and proposes

a practical, layered framework that a Bombay-based small or mid-sized firm can adopt without needing a full-time Chief Information Security Officer (CISO).

Why CA Firms Are Prime Targets

i. The Data Profile of a CA Firm

CA firms sit at a unique junction in the economic system. They deal not only with numbers but with structured, verified information about individuals, businesses, and transactions. Typical firm repositories include tax returns, financial statements, trial balances, bank statements, KYC records, loan documents, projections, valuation reports, and working papers. In many cases, firms also handle copies of PAN, Aadhaar, cancelled cheques, and, increasingly, one-time access to client portals.

From a criminal's perspective, this is exceptionally valuable raw material. With a single client file, an attacker may be able to construct a complete personal or business profile for identity theft, targeted social-engineering scams, or fraudulent borrowing. At the corporate level, access to draft financials, M&A plans, and internal board papers can support insider trading, corporate espionage, or extortion attempts. Unlike random customer lists breached from e-commerce sites, data held by CAs is curated and trusted, which increases its "market price" in underground forums.

ii. Misconceptions in Small and Mid-Sized Practices

Despite this exposure, many small and mid-sized firms believe that "we are too small to be on anyone's radar" or that "hackers will only target banks and large corporates".

However, attackers often prefer entities with weaker defences, especially where the data value per target is high. International and Indian experience shows that SMEs and professional firms are frequently targeted because they tend to have:

- Limited budgets for security tools and skilled IT staff.
- Fragmented infrastructure with a mix of old and new devices and software.
- Informal practices such as shared passwords, uncontrolled USB usage, and unencrypted laptops.

iii. Remote and Hybrid Work: The Vanishing Perimeter

Remote and hybrid work, accelerated during the pandemic and now normalized, has dissolved the traditional “office perimeter” guarded by a firewall. Partners and staff routinely access client data from home networks, personal laptops and tablets, and mobile phones on the move. Wi-Fi routers at home may still run default passwords; family devices may share the network; sensitive emails may be checked over open hotel Wi-Fi.

This shift means that security can no longer rely on the idea of a single safe network. Every endpoint and every identity used



“If a firm stores tax returns and financials on unencrypted laptops with shared passwords or uses free file-sharing platforms without access control, it may be difficult to argue that “reasonable care” was exercised when a breach occurs.”

to access client data becomes part of the attack surface. Without basic measures such as VPNs, hardened devices, and multi-factor authentication (MFA), remote access significantly increases the chance that a compromised device, stolen password, or unsafe network opens a backdoor into the firm’s environment.

Anatomy of Today’s Cyber Threats to CA Firms

i. Phishing, Spoofing and Business Email Compromise

Phishing remains the single most common starting point for cyber incidents in professional firms. Attackers craft emails that appear to come from trusted entities—such as the Income Tax Department, GSTN, MCA, RBI-regulated lenders, or even large clients—and send them in bulk, often timed around deadlines when staff are under pressure.

Common patterns include:

- Notices claiming discrepancies in an income-tax return with a link to “view order,” which actually leads to a credential-harvesting page.
- Messages from “bank relationship managers” seeking confirmation of client account details or sending “revised RTGS forms” with malware attachments.

- Emails apparently from a client CFO or partner asking for an urgent payment to a new vendor account or for sharing sensitive MIS reports through a shared link.

Once a user clicks a malicious link or enters credentials, attackers may gain full access to that mailbox. They then quietly monitor and forward emails, reset passwords on linked cloud services, and send convincingly timed messages to other staff and clients to initiate frauds—this is typically termed Business Email Compromise (BEC).

ii. Malware and Ransomware

Malware is a broad term that includes viruses, trojans, and, increasingly, ransomware. In ransomware incidents, the attacker encrypts the firm’s data and demands a ransom (often in cryptocurrency) to provide the decryption key. Modern ransomware operations often combine this with data exfiltration: they first copy out sensitive data and then encrypt systems, threatening to publish the stolen information if the ransom is not paid.

For a CA firm in peak filing or audit season, ransomware can be catastrophic. Access to trial balances, audit files, GST workings, and emails may be lost overnight. Even if backups exist, recovery may take days, during which staff are unable to work effectively, clients become anxious, and statutory deadlines may be missed. Moreover, if client data has been stolen, the firm must consider disclosure, contractual obligations, and reputation management in addition to restoration.

iii. Social Engineering and “Jamtara-Style” Attacks

Not all attacks rely on sophisticated code. Many simply exploit human psychology—authority, urgency, trust, or fear. Indian media and law-enforcement reports show how “Jamtara-style” call-centre frauds



and organized cybercrime rings use phone calls, SMS, WhatsApp, and social media to deceive educated professionals.

Examples relevant to CA firms include:

- Callers posing as bank officials or payment-gateway staff seeking OTPs “to reverse a failed transaction” relating to professional fees.
- Imposters claiming to be from client IT departments asking for VPN or email passwords “to fix an issue”.
- Attackers impersonating a partner on WhatsApp—using a downloaded profile photo—to ask a team member to urgently buy high-value gift vouchers or transfer funds.

Because these attacks bypass technical controls, awareness and verification discipline (for example, calling back on known numbers) are essential defences.

iv. Silent Data Exfiltration and Credential Theft

While ransomware and BEC are visible, many damaging breaches begin with silent data theft. Infostealer malware and keyloggers installed through malicious attachments or cracked software can capture passwords, browser-stored credentials, and even screenshots. Each time a staff member logs into a tax portal, internet banking, or

a cloud accounting system, their credentials may be sent to a remote command-and-control server.

Over weeks or months, attackers may accumulate working papers, client lists, and authentication data without triggering obvious alarms. The first sign might be a client’s bank account being misused, tax refunds diverted, or confidential financials appearing in a competitor’s hands.

v. Insider and Third-Party Risks

Insider risks cover a spectrum—from deliberate theft of client lists by departing staff to well-meaning employees forwarding sensitive data to personal email for “working from home”. In firms with weak access controls, a junior staff member might have wide-ranging read access to multiple clients’ folders, increasing impact if their account is misused.

Third-party risks arise when firms use outsourced book-keeping teams, freelance staff, or external IT vendors who have access to systems and data. Compromise of a remote-desktop solution, an unmanaged device used by an outsourced accountant, or lax security at an IT vendor can create a breach path into an otherwise well-controlled firm.

Professional, Legal and Ethical Dimensions

i. Confidentiality, Due Care and the ICAI Code of Ethics

The ICAI Code of Ethics requires members to maintain the confidentiality of information acquired as a result of professional and business relationships and not to disclose such information without proper authority unless there is a legal or professional duty to do so. This obligation implies not only avoiding intentional disclosure but also exercising reasonable care to prevent unauthorized access.

If a firm stores tax returns and financials on unencrypted laptops

with shared passwords or uses free file-sharing platforms without access control, it may be difficult to argue that “reasonable care” was exercised when a breach occurs. In some fact patterns, a serious, preventable cyber incident could raise questions around professional competence and due diligence, particularly where clients suffer direct loss.

ii. IT Law, Contracts and Client Expectations

Indian law also expects “reasonable security practices”. The Information Technology Act, together with its rules on sensitive personal data and subsequent data-protection developments, impose obligations on entities that process financial and personal information to implement appropriate security controls.

Separately, clients—especially banks, NBFCs, listed companies, and multinationals—are increasingly embedding data-protection and breach-notification clauses in engagement letters and vendor contracts. These may require CA firms to:

- Protect data using specified security standards.
- Restrict sub-processing or offshore storage.
- Notify clients within a defined time-frame if a breach affecting their data occurs.

Failure to comply can lead to termination of engagement, claims for damages, and reputational escalation within the client group.

iii. Cyber Insurance – Help, not a Panacea

Cyber-insurance products for SMEs and professional firms have grown in India, offering coverage for forensics, legal expenses, incident response, extortion support, and sometimes business interruption. However, insurers generally impose minimum security baselines and may deny or limit claims if the insured has ignored

basic controls, misrepresented its posture, or failed to patch known critical vulnerabilities.

For CA firms, insurance should be viewed as a risk-transfer tool after foundational controls are in place. It may be particularly relevant where clients or foreign group entities expect evidence of financial resilience in case of cyber incidents.

A Practical Cybersecurity Framework for CA Firms

For readers, the most valuable discussion is “What exactly should a firm do?” The following framework is designed for small and mid-sized firms that may not have a dedicated Chief Information Security Officer (CISO) but can invest in disciplined practices and appropriate external support.

i. Governance and Policy

Cybersecurity must start with governance, not gadgets. Partners should:

- Explicitly assign responsibility for information security—either to a partner or a small committee—while retaining overall accountability.
- Maintain a simple risk register listing key digital assets (email, cloud drives, tax and audit tools, practice-management systems), main threats, and existing controls.
- Adopt a concise written Information Security Policy that covers acceptable use of devices, password rules, handling of client credentials, remote-work conditions, and incident reporting.

The policy need not be lengthy, but it should be communicated, revisited annually, and supported by training and enforcement.

ii. Identity and Access Management

Identity is the new perimeter. Some practical steps:

- Implement MFA for firm email accounts, cloud storage,

practice-management tools, and VPN or remote-desktop access. Most mainstream platforms now support MFA at no extra cost.

- Avoid shared logins for staff; where a shared mailbox is needed (e.g., info@), use named accounts with delegated access.
- Apply the principle of least privilege: staff should have access only to clients and folders required for their engagements, and access should be promptly revoked when roles change or employment ends.

Periodic (for example, quarterly) reviews of user accounts, especially for leavers and external vendors, reduce “orphaned” access that attackers can exploit.

iii. Endpoint and Network Security

Because staff often work from multiple locations, firm devices must be hardened:

- Standardise on licensed operating systems and applications, with automatic patching turned on for OS, browsers, and office suites. Critical accounting and tax tools should be monitored for updates as vendors release security fixes.
- Install reputable endpoint-protection software (antivirus/EDR) and configure regular scans, web-filtering, and blocking of known malicious domains.
- Enable full-disk encryption on laptops and portable devices; enforce screen-lock and inactivity timeouts. Lost or stolen devices without encryption are a major breach vector.

On networks:

- Use business-grade routers where possible; change default passwords and update firmware.
- Segment guest Wi-Fi from internal networks at the office.

“For CA firms, insurance should be viewed as a risk-transfer tool after foundational controls are in place. It may be particularly relevant where clients or foreign group entities expect evidence of financial resilience in case of cyber incidents.”

- Require VPN connections when accessing firm resources from outside. Even simple, commercial VPN solutions can significantly improve security over open Wi-Fi.

iv. Data Classification, Encryption and Handling

Not all data requires the same level of protection. A simple classification scheme—such as public, internal, confidential, and highly confidential—helps align controls with risk. For example:

- Public: published articles, marketing material.
- Internal: HR policies, general internal communication.
- Confidential: normal client working papers, tax computations.
- Highly confidential: draft financials of listed entities, M&A deals, investigation reports, board papers.

For confidential and highly confidential data:

- Use secure sharing platforms with access control and, where possible, watermarking and download restrictions. Avoid sending large volumes of sensitive data as unencrypted email attachments.



- Ensure encryption in transit (HTTPS/TLS) is in place for portals and sharing tools; for very sensitive items, use password-protected archives shared through separate channels.
- Put clear rules around copying firm data to personal devices or external USB drives and consider technical controls to restrict or log such actions.

v. **Backup, Business Continuity and Incident Response**

Backups are the last line of defence against ransomware and accidental deletion. For CA firms, they should be non-negotiable. Recommended practices include:

- Follow the 3-2-1 rule: keep three copies of data, on two different media, with one copy offsite or in immutable cloud storage.
- Automate backups for critical file shares, cloud drives, and practice-management databases, and test restoration regularly to ensure that backups are not only present but usable.
- Define which systems are most critical (for example, audit files, tax working papers, emails) and set realistic Recovery Time Objectives (how fast they must

be restored) and Recovery Point Objectives (how much data loss in hours or days is tolerable).

An Incident Response Plan, even a simple two-page document, should outline:

- Who to inform first when suspicious activity is noticed.
- Immediate steps to contain impact (disconnecting devices, resetting passwords, preserving logs).
- External contacts—IT vendor, cyber forensic support, legal advisor, and, where relevant, client contact points and law-enforcement portals such as the National Cyber Crime Reporting Portal.

Practising this plan through a tabletop exercise once a year can significantly improve response effectiveness.

The Human Firewall: People, Culture and Training

Many high-profile cyber incidents ultimately trace back to human action—clicking a malicious link, using a weak password, forwarding data insecurely, or ignoring early warning signs. For CA firms, investing in people and culture often yields the highest return on effort.

Effective measures include:

- Periodic awareness sessions held every few months, focusing on real-world cases such as recent tax-related phishing scams or “Jamtara-style” frauds, instead of generic theoretical content.
- Simulated phishing exercises, where staff receive mock phishing emails and immediate feedback, to build pattern recognition.
- Clear “dos and don’ts” documented in a simple user guide: how to verify unexpected payment requests, what to do if you suspect malware, and which channels to use for sharing different types of data.

Most importantly, firms should encourage a no-blame reporting

culture. Staff should feel safe admitting that they clicked a suspicious link or shared data incorrectly, so the firm can respond quickly and limit damage. Punitive reactions or ridicule discourage reporting and allow incidents to escalate.

Vendors, Cloud, and the Wider Ecosystem

i. **Managing IT Vendors and SaaS Tools**

Given that many firms rely on cloud-based accounting, practice-management, document-sharing, and backup tools, vendor risk must be actively managed. Practical steps include:

- Reviewing contracts to ensure they address data security, sub-processors, data-location (where information is stored), and incident-notification timelines.
- Asking SaaS providers for evidence of security posture, such as ISO 27001 certification or SOC 2 reports, where appropriate for the firm’s risk level and client expectations.
- Limiting and periodically reviewing access granted to external IT support staff; terminating access when projects end, or vendors change.

ii. **Learning from Professional and Peer Networks**

Professional forums and peer networks are increasingly



addressing themes such as cybercrime, digital practice, and technology risks through articles, webinars, and study-circle discussions. Engaging with this ecosystem enables firms to:

- Benchmark their preparedness against peers.
- Learn from anonymised case studies of incidents and near-misses.
- Access curated resources, sample policies, and checklists developed by practitioners with IT-risk expertise.

As attacks continue to evolve, staying connected to such professional communities helps firms avoid learning “the hard way” through their own breaches.

From Compliance Burden to Competitive Advantage

Many firms still view cybersecurity as a regulatory or client-driven burden—something to be handled minimally to “tick the box”. However, there is an emerging opportunity to reposition strong information security as a differentiator.

Clients, particularly sophisticated corporates and international groups, increasingly ask how their data will be protected and may favour advisors who can articulate a clear posture. Firms with demonstrable controls—documented policies, MFA, tested backups, staff



“Firms should encourage a no-blame reporting culture. Staff should feel safe admitting that they clicked a suspicious link or shared data incorrectly, so the firm can respond quickly and limit damage. Punitive reactions or ridicule discourage reporting and allow incidents to escalate.”

training, and incident-response readiness—are better placed to win and retain high-sensitivity mandates such as forensic assignments, insolvency, internal investigations, and transaction support.

For readers, building mid-sized practices, including a brief, plain-language description of the firm’s security approach in proposals and on websites, can reinforce a message of trust and professionalism, provided it accurately reflects practice. Cyber-resilience then becomes not just a shield against loss, but a positive attribute of the firm’s brand.

The Digital Personal Data Protection Act, 2023 (DPDP Act)

The Digital Personal Data Protection Act, 2023 (DPDP Act), enacted on August 11, 2023, establishes India’s first comprehensive framework for safeguarding digital personal data while balancing individual privacy rights with legitimate data processing needs of businesses and government entities. It defines key roles such as Data Principals (individuals whose data is processed), Data Fiduciaries (entities controlling data), and Significant Data Fiduciaries (those handling large volumes or sensitive data), mandating consent-based processing—free, specific, informed, and unconditional—or legitimate uses, alongside obligations like data security, breach notifications,



and grievance redressal. The Act establishes the Data Protection Board of India to enforce compliance, monitor breaches, and impose penalties up to ₹250 crore, with exemptions for personal/domestic use and public data, and restrictions on cross-border transfers to notified countries. Special protections apply to children’s data, prohibiting tracking or targeted advertising without verifiable parental consent.

The Digital Personal Data Protection (DPDP) Rules, 2025

The Digital Personal Data Protection (DPDP) Rules, 2025 explain how the DPDP Act, 2023 has to be followed in day-to-day practice. They were issued in November 2025 and laid down simple rules on how to take consent, what basic security measures to use (like access control, encryption, logs, and backups), and how quickly data breaches must be reported to both affected individuals and the Data Protection Board. For CA and audit firms, these Rules mean clearer expectations that firms should have written procedures, control over their IT vendors, and evidence that they are using reasonable security practices for client data.

Cybersecurity Asset Management for CA Firms

Cybersecurity asset management is, at its core, about knowing exactly what technology your CA firm uses and how it is protected. This means keeping a live, structured list of all laptops,

desktops, servers, Wi-Fi routers, mobile phones, cloud applications, e-filing portals, and the locations where client tax, audit, and finance data are stored. Each of these assets is a potential entry point for an attacker, so having this visibility allows the firm to see which systems are critical, which ones are outdated, and where basic safeguards—like patches, antivirus, encryption, or access controls—are missing.

In practical terms, firms can tag important assets (for example, folders containing working papers of listed entities or shared drives with PAN/Aadhaar details) as “high-risk”, and then ensure they are monitored more closely, updated promptly, and accessed only by authorised users. The same inventory helps identify “forgotten” machines, shadow IT tools, or unmanaged home devices that often become weak spots in ransomware or data-breach incidents, especially in remote and hybrid work models.

For small and mid-sized practices that do not have a full-time Chief Information Security Officer (CISO), building basic discipline around asset management—clearly assigning ownership for key systems, scheduling simple quarterly reviews, and using modest automation to detect new or unpatched devices—offers a very practical way to demonstrate “reasonable security practices” under IT and data-protection laws. At the same time, it materially improves the firm’s ability to prevent, detect, and respond to cyber incidents, thereby protecting



“The profession’s social licence ultimately rests on trust—trust that CAs will handle financial and personal information with integrity, competence, and care. In a digital and remote-first world, that trust now extends to the robustness of firms’ cybersecurity practices.”

client data and supporting long-term trust in the practice.

Conclusion: Building a Cyber-Resilient Profession

The profession’s social licence ultimately rests on trust—trust that CAs will handle financial and personal information with integrity, competence, and care. In a digital and remote-first world, that trust now extends to the robustness of firms’ cybersecurity practices.

For CA firms across India, cyber threats are inevitable—the real question is whether they are prepared when they strike. By elevating cyber risk to a core practice-management priority, embedding it firmly in governance, and fortifying technical and human defences, firms can master the digital landscape with unshakeable confidence.

For CA firms, cybersecurity goes far beyond IT spend—it is the essential base on which professional excellence and long-term resilience of the practice truly rest.

References

- Ministry of Electronics and Information Technology (MeitY). *The Digital Personal Data Protection Act*, 2023. <https://www.meit.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef-35e82c42aa5.pdf>



- Press Information Bureau (PIB). *DPDP Rules, 2025 Notified* (14 November 2025). <https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=156054&ModuleId=3>
- PRS Legislative Research. *The Digital Personal Data Protection Bill*, 2023. <https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023> (Updated January 2026)
- Institute of Chartered Accountants of India (ICAI). *Code of Ethics* 2019. <https://nagpuricai.org/seminar-presentations/Code-of-Ethics-1.pdf>
- Ministry of Electronics and Information Technology. *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules*, 2011. <https://www.dataguidance.com/sites/default/files/in098en.pdf>
- Tanium. *What is Cybersecurity Asset Management (CSAM)?* (April 2025). <https://www.tanium.com/blog/what-is-cybersecurity-asset-management-csam/>
- Lansweeper. *How Cybersecurity Asset Management Enhances Your Security*. <https://www.lansweeper.com/blog/cybersecurity/how-cybersecurity-asset-management-enhances-your-it-security/> (August 2025)
- ICAI. *Cybersecurity & Data Privacy in GCCs* (GCC Summit Presentation, June 2025). <https://gcc.icai.org/wp-content/uploads/2025/07/Alok-Gupta-GCC-Summit-28-6-25.pdf>

Author may be reached at
peeyushsharmaca@gmail.com
and eboard@icai.in