# Data Privacy & Cybersecurity: A Governance Imperative

Relating with the theme of 'Sabka Vikas', 'Surakshit Vikas', this article enumerates the significance of secure access to data in this digitalized world. Cybersecurity is a key concern and its implementation in organisations is not only the responsibility of IT professionals but also governance professionals like company secretaries.

**CS Rajiv Malik, ACS**
Legal Leader (DGM)
LG Electronics India Ltd. Greater Noida
*rajiv.malik@lge.com*

## INTRODUCTION

*"Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet." – Gary Kovacs*

This year's Union Budget, themed "Sabka Vikas" (everyone's growth), emphasizes inclusive development. However, true inclusion in our increasingly digital economy requires not just access, but also secure access. "Surakshit Vikas" (secure growth) is therefore paramount. Without robust data protection and cybersecurity, the benefits of digitalization risk being undermined by fraud, data breaches, and a loss of trust, disproportionately impacting vulnerable populations. Recognizing this connection, the Ministry of Electronics and Information Technology (MeitY) has significantly increased funding for the Data Protection Board of India (DPBI), a 2.5-fold rise from previous allocations. Coupled with an 18% increase in the cybersecurity budget, this underscores the government's commitment to bolstering the nation's digital defenses. However, while these nationwide measures are essential, the ultimate responsibility also lies with corporations. Are businesses taking similarly proactive steps to integrate data privacy and cybersecurity into their core culture? In today's interconnected world, this is no longer a discretionary initiative, but a mandatory one for survival and success.

The ancient wisdom of the Ramayana offers a striking parallel to the data privacy challenges we face today. Vibhishana's act of revealing the secret of Ravana's vulnerability—his *nabhi*—led to the fall of Lanka. This timeless story encapsulates the modern-day risks of insider threats and information leaks. In the corporate landscape, a single breach—whether originating from a malicious insider, a sophisticated cyberattack, or simply poor data governance—can dismantle years of hard-won trust, jeopardize financial stability, and irrevocably damage corporate reputation. Just as Ravana's mighty fortress could not protect him once his critical weakness were exposed, even the most technologically fortified organizations remain vulnerable if their data is not adequately secured. This raises a crucial question: Will businesses proactively safeguard their digital "Lanka," or will they, like Ravana, succumb to their own internal and external vulnerabilities?

This article will delve into the multifaceted challenges corporations face in ensuring data privacy and combating the ever-evolving landscape of cyber threats. Furthermore, it will highlight the pivotal and increasingly important role of the company secretary in strengthening data governance frameworks, fostering a culture of regulatory compliance, and ultimately safeguarding the organization's digital future in an increasingly perilous cyber environment.

## REGULATORY COMPLIANCE FRAMEWORK

In the modern digital economy, data privacy and cybersecurity are not just best practices—they are legal imperatives. Governments worldwide are tightening regulations to protect personal and corporate data, imposing stringent compliance requirements on businesses.

**India's Data Protection Laws:**

India has recently enacted significant regulations to strengthen data privacy and cybersecurity within the country:

1. **The Digital Personal Data Protection Act (DPDP Act), 2023:**
   - Establishes fundamental rights for individuals over their personal data, including the right to access, correct, and erase their data.
   - Mandates explicit consent for the collection and processing of personal data.
   - Imposes significant penalties for data breaches and non-compliance (up to ₹250 crore per violation).

- Establishes the Data Protection Board of India (DPBI) to oversee compliance with the DPDP Act and enforce its provisions.

2. **The Information Technology (IT) Act, 2000 & CERT-In Guidelines:**
   - Governs various aspects of cybersecurity, including electronic transactions, digital evidence, and cybercrime.
   - Mandates the reporting of cybersecurity incidents to CERT-In (Indian Computer Emergency Response Team) within a strict timeframe.
3. **Sector-Specific Regulations:**
   - **RBI's Data Localization Norms:** Requires financial institutions to store Indian customers' data within the geographical boundaries of India.
   - **SEBI's Cybersecurity Framework:** Mandates stock exchanges and other market participants to implement robust cyber resilience frameworks to protect against cyber threats.
   - **IRDAI Information and Cyber Security Guidelines, 2023:** Focus on ensuring that insurance companies implement robust information security practices, conduct regular risk assessments, and adhere to industry standards to safeguard against cyber threats and breaches. The guidelines also emphasize the need for effective data protection and privacy measures to ensure the confidentiality, integrity, and availability of policyholders' information.

## GLOBAL DATA PROTECTION LAWS

1. **EU's General Data Protection Regulation (GDPR):** Widely considered the gold standard in data protection, GDPR imposes strict consent requirements, comprehensive data breach notification rules, and substantial fines for non-compliance (up to €20 million or 4% of annual turnover).
2. **United States' Sectoral Approach:** Unlike GDPR's comprehensive approach, the U.S. follows an industry-specific model, with laws such as:
   - **California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA):** Grants California residents significant rights over their personal data, including the right to know what data is being collected, the right to delete their data, and the right to opt-out of the sale or sharing of their personal information.
   - **Health Insurance Portability and Accountability Act (HIPAA):** Governs the privacy and security of protected health information (PHI) within the healthcare industry.
   - **Gramm-Leach-Bliley Act (GLBA):** Regulates financial institutions' data security and privacy practices.
3. **China's Personal Information Protection Law (PIPL):** One of the strictest data protection laws globally, PIPL mandates data localization, imposes strict cross-border data transfer restrictions, and prescribes severe penalties for mishandling Chinese citizens' data.

## THE EXPANDING CYBER THREAT LANDSCAPE

In today's hyper-connected world, businesses are no longer just competing for market share—they are also locked in a constant, often invisible battle against a wide range of cyber threats. As data becomes increasingly valuable, cybercriminals, state-sponsored hackers, and malicious insiders have ramped up their attacks, making cybersecurity an urgent, non-negotiable priority for organizations across the globe. Unlike traditional threats, which were often physical and localized, today's cyber threats are sophisticated, constantly evolving, and capable of causing unparalleled financial and reputational damage on a global scale.

- **The Dark Side of Digital Transformation**

  The rapid and often necessary shift towards cloud computing, the increasing prevalence of remote work arrangements, have unlocked incredible efficiencies and opportunities for businesses. However, this digital transformation has also inadvertently widened the attack surface for cybercriminals. Organizations now store vast amounts of highly sensitive data—including customer information, valuable intellectual property, critical financial records, and confidential trade secrets—making them increasingly lucrative targets for a wide range of cyberattacks. A single, seemingly insignificant vulnerability in an organization's network can expose millions of records, potentially leading to severe regulatory penalties, significant financial losses, and, perhaps most damaging of all, a catastrophic loss of stakeholder trust.

  The question is no longer *if* a cyber incident will occur, but rather *when* it will happen. Cybercriminals are continuously adapting their methods, leveraging cutting-edge technologies like AI and machine learning to bypass traditional security defenses and stay one step ahead of those trying to protect valuable data. This constant evolution necessitates a proactive and highly strategic approach from governance professionals, and particularly Company Secretaries, who now play a pivotal role in shaping their organization's overall cyber resilience and its ability to withstand and recover from attacks.

- **AI and Cyber Threats**

  Artificial intelligence (AI) has revolutionized the field of cybersecurity by enabling faster and more accurate threat detection, facilitating automated response mechanisms, and providing powerful predictive analytics. However, the very same AI technology is also being weaponized by cybercriminals. AI-powered malware, highly convincing deepfake phishing

attacks, and sophisticated automated hacking tools have made cyber threats more dangerous and difficult to defend against than ever before. Attackers can now use machine learning algorithms to effectively evade detection, convincingly mimic legitimate users, and exploit vulnerabilities with pinpoint precision.

For instance, cybercriminals have begun deploying deepfake technology to impersonate high-level executives in video conference calls, tricking unsuspecting employees into transferring funds or sharing confidential data under false pretenses. Similarly, AI-driven ransomware-as-a-service (RaaS) platforms have enabled even non-technical criminals to launch highly sophisticated cyberattacks at scale, democratizing cybercrime and making it accessible to a wider range of malicious actors. The challenge for governance professionals is to stay ahead of these rapidly evolving threats by integrating AI-driven security measures while simultaneously ensuring full compliance with evolving data protection laws and regulations.

- **Ransomware Attacks**

One of the most alarming and prevalent cyber threats facing businesses today is ransomware—malicious software that encrypts an organization's critical data and demands a ransom payment, often in cryptocurrency, for its release. Ransomware attacks have evolved significantly from indiscriminate mass infections to highly targeted operations, where cybercriminals meticulously research their victims to identify their most valuable data assets and maximize the potential impact of the attack. They often focus on organizations that are heavily reliant on their data and cannot afford extended downtime, such as hospitals, financial institutions, and government agencies.

> While organizations must prioritize strengthening their cybersecurity defenses, they must also ensure that these security measures do not unduly hinder operational efficiency or negatively impact the customer experience.

Consider, for example, the infamous WannaCry ransomware attack in 2017, which affected over 200,000 computers across 150 countries, crippling hospitals, disrupting banking operations, and even impacting government agencies. Closer to home, Indian companies have also fallen victim to large-scale ransomware incidents, with attackers demanding substantial payments in cryptocurrencies to restore access to critical data and systems.

The consequences of a ransomware attack extend far beyond immediate financial losses. They can severely disrupt business operations, inflict significant damage to a company's reputation, and, in some cases, lead to long-term legal liabilities. Organizations that fail to implement robust and multi-layered cybersecurity measures risk losing not just money, but also the trust of their customers, the confidence of their stakeholders, and potentially their competitive advantage.

- **State-Sponsored Cyber Attacks**

In the increasingly complex geopolitical landscape, cyber warfare has emerged as a powerful tool for espionage, sabotage, and economic disruption. Governments and intelligence agencies are actively engaging in cyber operations to target foreign corporations, critical infrastructure, and even financial institutions. These attacks are often designed to steal sensitive information, disrupt essential services, or gain a strategic advantage.

For instance, APT (Advanced Persistent Threat) groups, often linked to nation-states, have been known to infiltrate multinational corporations, stealing sensitive trade secrets, valuable intellectual property, and confidential research data. These attacks are frequently sophisticated, prolonged, and extremely difficult to detect, making them a significant concern for governance professionals responsible for handling confidential corporate data. The attribution of these attacks can also be challenging, often blurring the lines between state-sponsored activity and sophisticated cybercriminal operations.

- **Data Breaches**

One of the most devastating consequences of cyber threats, and one that resonates deeply with the public, is the occurrence of data breaches. When an organization's sensitive data, particularly personal information, falls into the wrong hands, the damage is often irreversible. High-profile data breaches have exposed the personal information of millions of people, leading to regulatory fines, costly lawsuits, and irreparable reputational harm. The erosion of trust that follows a data breach can be particularly difficult to recover from.

## THE INVISIBLE THREAT: INSIDER RISKS AND HUMAN FACTORS

While organizations often invest heavily in sophisticated firewalls, advanced encryption technologies, and AI-driven cybersecurity tools to guard against external hackers, they frequently underestimate the most insidious and often overlooked threat—insiders with legitimate access to sensitive data. A disgruntled employee, a negligent staff member, or even a well-meaning executive unaware of fundamental security protocols can inadvertently become the weakest link in an organization's cybersecurity framework. It's a difficult truth, but sometimes the greatest threat comes from within – *ghar ka bhedi Lanka daheye.* Insider risks are particularly dangerous and difficult to detect because they originate from trusted sources—people who already have legitimate access to critical systems and sensitive information.

- **Why Insider Threats Are Harder to Detect**

  Unlike external cyberattacks, which often leave unusual digital footprints and trigger security alerts, insider threats frequently appear as normal, everyday activity within the organization's systems. A finance executive downloading a spreadsheet, an HR manager accessing personnel records, or an IT administrator modifying access controls—these actions can seem perfectly routine until a breach is discovered and the true extent of the damage becomes apparent.

  This inherent difficulty in distinguishing between legitimate activity and malicious behavior makes it absolutely essential for organizations to develop robust strategies to effectively detect, deter, and mitigate insider risks without unduly compromising employee trust or hindering operational efficiency.

- **Insider Threats Are a Governance Challenge, Not Just an IT Issue**

  The most sophisticated and technologically advanced cybersecurity system can be rendered ineffective if insider threats are ignored or underestimated. Whether motivated by malicious intent or simply the result of human error, insiders can cause catastrophic data breaches, inflicting significant financial losses, reputational damage, and legal liabilities. Governance professionals must champion the development and implementation of risk-aware policies, cultivate a strong security culture throughout the organization, and ensure the use of ethical monitoring practices to effectively protect organizations from this often invisible and highly damaging threat. Insider risk management is not solely an IT issue; it is a fundamental governance challenge that requires the active involvement and leadership of company secretaries and other governance professionals.

## DATA PRIVACY VS. CYBERSECURITY: A GOVERNANCE PROFESSIONAL'S PERSPECTIVE

In the digital era, two terms frequently dominate boardroom discussions and strategic planning sessions: data privacy and cybersecurity. While often used interchangeably, they are distinct yet interconnected concepts that require different yet complementary approaches. Data privacy governs how personal and sensitive information is collected, stored, used, and shared, ensuring that individuals have control over their own data and that organizations handle it responsibly and ethically. Cybersecurity, on the other hand, focuses on protecting systems, networks, and data from unauthorized access, malicious attacks, and data breaches.

For governance professionals, and particularly Company Secretaries, understanding the nuanced relationship between data privacy and cybersecurity is absolutely crucial. Their role is no longer confined to ensuring regulatory compliance; they must now act as strategic advisors on corporate data governance strategies, proactively mitigate cyber risks, and ensure the ethical handling of sensitive information throughout the organization. The challenge lies in striking a delicate balance—protecting data without unduly stifling business innovation or hindering legitimate data-driven initiatives.

## UNDERSTANDING THE DIFFERENCE: WHY IT MATTERS FOR GOVERNANCE PROFESSIONALS

To fully appreciate the crucial distinction between data privacy and cybersecurity, consider the following analogy:

- **Cybersecurity is like building a robust fortress:** It involves deploying firewalls, implementing strong encryption protocols, and establishing comprehensive security procedures to prevent unauthorized access to sensitive information and protect against external attacks.
- **Data privacy is like setting and enforcing the rules *within* the fortress:** It ensures that even within a secure environment, data is accessed, processed, and shared responsibly, ethically, and in strict accordance with relevant regulatory guidelines and legal requirements.

Both aspects are inextricably linked and interdependent. A company may invest heavily in strong cybersecurity measures, effectively building a seemingly impenetrable fortress. However, if it collects excessive personal data without explicit user consent, or if it shares data with third parties without proper authorization, it is in clear violation of data privacy laws and regulations. Conversely, an organization may have the most stringent and well-intentioned data privacy policies in place, but without adequate cybersecurity measures to protect that data from breaches, those policies become meaningless and unenforceable.

For governance professionals, understanding both domains is absolutely critical to ensuring overall corporate resilience in the digital age. Data breaches can result in significant legal liabilities, substantial financial losses, and irreparable damage to an organization's reputation, making it imperative for company secretaries to play a proactive and strategic role in all aspects of data governance.

## THE COST OF NON-COMPLIANCE: LEGAL AND REPUTATIONAL RISKS

Failing to comply with data protection laws and cybersecurity regulations can lead to a range of severe consequences, including:

- **Financial Penalties:** Regulatory fines for violations can be substantial, often running into millions of dollars, significantly impacting the organization's bottom line.

- **Operational Disruptions:** Regulatory investigations and enforcement actions can disrupt business operations, causing delays, inefficiencies, and potential losses.
- **Reputation Damage:** Loss of customer trust and damage to brand credibility can have long-term and often irreversible effects on the organization's reputation and market position.
- **Criminal Liability:** In extreme cases of negligence or intentional misconduct, CXOs and compliance officers can be held personally liable for data breaches or other cybersecurity violations.

Organizations that fail to prioritize data privacy and cybersecurity face severe and often far-reaching consequences. For governance professionals, these incidents serve as a critical wake-up call. Ensuring compliance is not simply about avoiding penalties; it is fundamentally about protecting corporate integrity, maintaining stakeholder trust, and preserving the long-term value of the organization.

## BRIDGING THE GAP: THE COMPANY SECRETARY'S ROLE IN DATA GOVERNANCE

Company Secretaries are uniquely positioned within organizations to effectively bridge the gap between cybersecurity and data privacy. Navigating this complex and ever-evolving regulatory environment requires a proactive, strategic, and highly informed approach. Their responsibilities typically include:

1. **Embedding Compliance in Corporate Strategy:**
    - Data privacy and cybersecurity should not be treated as mere legal checkboxes or afterthoughts—they must be fully integrated into the organization's overall strategic decision-making processes.
    - Company Secretaries should advise the Board of Directors on emerging regulatory developments, potential compliance risks, and recommend policies and procedures that align with evolving laws and best practices.
    - Implementing a Privacy by Design approach, where compliance is built into business processes, systems, and product development from the very outset, is absolutely crucial.
2. **Conducting Regulatory Audits and Gap Assessments:**
    a) Regular and thorough compliance audits can help identify gaps in data protection measures and potential vulnerabilities before regulators impose penalties or breaches occur.
    b) Gap assessments should focus on key areas such as:
        - **Consent mechanisms:** Are customers and employees providing informed and explicit consent for data collection and processing?

- **Data storage and retention policies:** Is the organization retaining data longer than legally permitted or necessary for business purposes?
- **Third-party vendor compliance:** Are the organization's partners and vendors also meeting the required regulatory standards and adhering to data protection best practices?

3. **Strengthening Data Governance Policies:**
   - Drafting and implementing comprehensive Data Privacy Policies (DPPs) that fully comply with both global and Indian regulations.
   - Developing and regularly updating Incident Response Plans to ensure rapid, coordinated, and effective action in the event of a data breach or cyberattack.
   - Conducting Data Protection Impact Assessments (DPIAs) for high-risk data processing activities to identify and mitigate potential privacy risks.
4. **Ensuring Cross-Border Data Compliance:**
   a) With business operations becoming increasingly global and interconnected, companies must comply with a complex web of cross-border data transfer regulations.
   b) Governance professionals should,
      - implement Standard Contractual Clauses (SCCs) or other appropriate legal mechanisms for international data transfers.
      - ensure data localization where required by law (e.g., under India's DPDP Act and other similar regulations).
      - stay informed and updated on new bilateral and multilateral data-sharing agreements and their potential impact on the organization.
5. **Cybersecurity Due Diligence in M&A and Partnerships:**
   a) Data privacy and cybersecurity risks are often overlooked in mergers and acquisitions (M&A) transactions, potentially leading to significant post-acquisition liabilities.
   b) Company Secretaries should:
      - Conduct thorough cyber risk assessments as part of the due diligence process before any acquisitions or mergers.
      - Ensure appropriate contractual indemnities for data breaches or cybersecurity incidents in vendor agreements and partnership arrangements.
      - Recommend cyber insurance coverage as an integral part of the organization's overall risk management strategies.
6. **Strengthening Employee Awareness and Training:**
   - Conduct mandatory and recurring cybersecurity training programs that focus on real-world case studies of insider threats and educate employees about best practices for data protection.
   - Implement simulated phishing attack exercises to regularly test employees' ability to recognize and avoid falling victim to phishing scams and other social engineering tactics.
   - Foster a security-first culture where employees feel a shared responsibility for data protection and are encouraged to report any suspicious activity.
   - Conduct regular access reviews to ensure that employees do not retain unnecessary privileges after role changes, promotions, or departures.
7. **Monitoring and Detecting Anomalous Insider Behavior:**
   a) Deploy User Behavior Analytics (UBA) tools that track and analyze user activity to identify anomalous behavior, such as:
      - Downloading or accessing unusually large amounts of data.
      - Logging in at odd hours or from unusual locations.
      - Accessing confidential information that is not related to their job responsibilities.
   b) Set up automated alerts to notify security personnel when employees attempt unauthorized data transfers or access restricted systems.
8. **Encouraging a Speak-Up Culture and Whistleblower Mechanisms:**
   - Create a safe and supportive environment where employees feel comfortable reporting suspicious behavior without fear of retaliation.
   - Establish anonymous reporting channels for ethical concerns related to data misuse or security violations.
   - Clearly communicate the consequences of policy violations, ensuring that both malicious insiders and negligent behavior are addressed promptly and consistently.
9. **Enforcing Data Loss Prevention (DLP) Mechanisms:**
   - Deploy DLP tools to detect and block unauthorized data transfers via email, cloud services,

USB devices, or other potential exfiltration channels.

- Implement robust encryption protocols for all sensitive files, ensuring that even if data is leaked, it remains unusable to unauthorized parties.
- Conduct regular audits of file-sharing activities to identify any abnormal patterns or potential data exfiltration attempts.

**10. Striking the Right Balance: Security vs. Accessibility**

While organizations must prioritize strengthening their cybersecurity defenses, they must also ensure that these security measures do not unduly hinder operational efficiency or negatively impact the customer experience. Excessively strict security protocols that slow down workflows or make it difficult for employees to access necessary information can lead to employee resistance, decreased productivity, and operational inefficiencies. On the other hand, excessive data collection without adequate safeguards exposes businesses to significant regulatory penalties and reputational risks.

Company Secretary Professionals must play a key role in helping companies find the right balance—implementing security measures that are both robust and user-friendly, ensuring full compliance without unnecessarily restricting business agility or hindering innovation.

## CONCLUSION

Data protection has become a global priority, with countries around the world implementing increasingly stringent privacy laws. India, too, is not immune to this shift, as the country aligns with global standards in advancing its own privacy regulations. This growing focus on data security has compelled companies worldwide to prioritize safeguarding their data more than ever before. In this evolving landscape, the Company Secretary, transitioning from a compliance officer to a strategic advisor, stands at the forefront of this effort. They guide the board, foster a culture of cyber resilience, and ensure that data governance is not just a policy or simply a box to tick, but a deeply ingrained organizational value. The Company Secretary, as a champion of good governance, plays a vital role in navigating this complex terrain, ensuring that *"Sabka Vikas –Surakshit Vikas"* is not just a vision, but a secure and sustainable reality for all.

## REFERENCES:

**Government website:**

*i.* **Digital Personal Data Protection Act, 2023**

*https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf*

*ii.* **Union Budget 2025-26**

*https://www.india.gov.in/spotlight/union-budget-2025-2026#:~:text=Budget%20Estimates%202025%2D26&text=The%20net%20tax%20receipts%20are,)%20earmarked%20in%20FY2025%2D26.*

*iii.* **The Information Technology (IT) Act, 2000**

*https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=#:~:text=%5B9th%20June%2C%202000%5D%20An,communication%20and%20storage%20of%20information%2C*

*iv.* **General Data Protection Regulation**

*https://gdpr-info.eu/*

*v.* **California Consumer Privacy Act (CCPA)**

*https://oag.ca.gov/privacy/ccpa*

*vi.* **The Health Insurance Portability and Accountability Act (HIPAA)**

*https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,Rule%20to%20implement%20HIPAA%20requirements.*

*vii.* **IRDAI Information and Cyber Security Guidelines, 2023**

*file:///C:/Users/janvi.sharma/Downloads/IRDAI%20CS%20Guidelines%202023.pdf*

**Other References:**

*viii. file:///C:/Cybersecurity-&-Data-Privacy-for-Indian-Businesses_-Strategies-&-Insights.pdf*

*ix. House of Commons House of Lords Joint Committee on the National Security Strategy A hostage to fortune: ransomware and UK national security First Report of Session 2023–24*

*https://committees.parliament.uk/publications/42493/documents/211438/default/*

*x. Personal data of nearly 8 million Angel One customers leaked online: sources*

*https://economictimes.indiatimes.com/tech/technology/personal-data-of-almost-8-million-angel-one-customers-leaked-online/articleshow /111612380.cms?from=mdr*

*xi. Equifax Data Breach Settlement*

*https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement*

*xii. All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*

*https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html*

*xiii. The case of Edward Snowden*

*https://www.whistleblowers.org/news/the-case-of-edward-snowden/*