INDUSTRIAL CYBER RISK MANAGEMENT: INTEGRATING INFORMATION TECHNOLOGY AND OPERATIONAL TECHNOLOGY SECURITY TO FULLY ADDRESS BUSINESS RISK

Zia Khan, Amity Law School Noida

ABSTRACT

The convergence of Information Technology (IT) and Operational Technology (OT) has transformed industrial operations by enhancing automation, connectivity, and efficiency. However, this integration has also increased cyber vulnerabilities, exposing critical infrastructure and industrial systems to serious threats affecting business continuity, public safety, and national security. This paper examines the cybersecurity risks arising from IT-OT integration and highlights the need for comprehensive industrial cyber risk management frameworks.

The paper analyzes India's legal and regulatory framework governing industrial cybersecurity, including the Information Technology Act, 2000, CERT-In Directions, the National Critical Information Infrastructure Protection Centre (NCIIPC), and the National Cyber Security Policy,

2013. It further examines the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025, focusing on obligations relating to data protection, security safeguards, and breach reporting in industrial environments. The study also discusses key judicial decisions that have shaped India's cybersecurity and privacy jurisprudence. The paper concludes that industrial cybersecurity must be treated not merely as a technical issue, but as an essential aspect of legal compliance, corporate governance, and national security.

I. INTRODUCTION

The growth of digital technologies has boosted a transformation across industries. Today, industries depend upon interconnected systems for managing operations, production, communication and other business processes. While this digital transformation has improved efficiency and productivity, it came at the cost of major cyber risks. The integration and collaboration of Information Technology (IT) and Operational Technology (OT) has created new vulnerabilities that affect not only business operations but also public safety, critical infrastructure and national security.

As a result, industrial cyber risk management has become an important and integral component of modern business governance. Organizations increasingly seek a unified approach that integrates IT and OT security frameworks to manage and reduce these cyber threats. This research paper examines the nature of IT-OT convergence risks, India's evolving legal and regulatory landscape, including the relevant acts and the legal framework in India, and the judiciary's role in shaping industrial cyber security obligations.

II. THE IT AND OT RELATIONSHIP

Information Technology refers to systems used for data processing, storage, communication, and business operations. IT systems primarily focus on confidentiality, integrity, and availability of data. Operational Technology consists of hardware and software systems used to monitor and control industrial operations and physical processes. OT systems include industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), and automated manufacturing systems.

Historically, IT and OT functioned separately. OT systems were isolated from external networks and relied on proprietary technologies, making them relatively secure from cyber attacks. However, with industrial digitization, remote monitoring, cloud computing, and the Industrial Internet of Things (IIoT), OT systems are increasingly connected to IT networks. This convergence has significantly increased cyber exposure.

III. THE GROWING CYBER RISK

The integration of IT and OT has expanded the attack surface for cybercriminals. A cyber attack on industrial systems can result in operational shutdowns, financial losses, theft of intellectual

property, environmental damage, and even threats to human life.

Several high profile cyber incidents have demonstrated the severe consequences of attacks on industrial infrastructure. Critical sectors such as energy, manufacturing, transportation, healthcare, and water supply are especially vulnerable. Since industrial operations are interconnected with national supply chains and critical infrastructure, disruptions can have widespread economic and social consequences.

Unlike traditional IT systems, OT environments prioritize operational continuity and safety. Even minor disruptions in industrial control systems can halt production processes or create hazardous conditions. Therefore, industrial cyber security requires a different approach from conventional IT security.[1]

IV. INDIA'S LEGAL FRAMEWORK

India views industrial cyber security as a matter of national security. With increasing digitization in sectors such as power, oil and gas, transportation, telecommunications, banking, healthcare, and manufacturing, India has recognized the urgent need to integrate IT and OT security frameworks. The government has emphasized that cyber security must be treated as a business risk rather than merely an IT problem.

a) The Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) is the foundational legislation governing cyber security and electronic commerce in India. Section 43A of the IT Act imposes liability on organizations that handle sensitive personal data and fail to maintain "reasonable security practices and procedures," making them liable to pay compensation to affected individuals.[2] Section 66F creates the offence of cyber terrorism which refers to the targeting critical information infrastructure with intent to threaten India's unity, integrity, security, or sovereignty and provides for imprisonment for life.[3] Section 70 empowers the Central Government to designate any computer resource a "protected system," and any unauthorized

[1] Naveen Joshi, *Industrial Cyber Risk Management: Integrating IT and OT Security to Fully Address Business Risk*, Forbes Tech Council (Feb. 13, 2023) https://www.forbes.com/councils/forbestechcouncil/2023/02/13/industrialcyber-risk-management-integrating-it-and-ot-security-to-fully-address-business-risk/

[2] The information technology (amendment) act 2008, Section 43A

[3] The information technology (amendment) act 2008, Section 66F

access to such systems is a criminal offence. These provisions are particularly significant for industrial environments where OT systems underpin critical national infrastructure.[4]

b) CERT-In and Mandatory Incident Reporting

The Indian Computer Emergency Response Team (CERT-In), established under Section 70B of the IT Act, is the national nodal agency for responding to cyber security incidents. CERT-In's 2022 Directions mandate that all organizations including service providers, intermediaries, data centers, and businesses operating critical infrastructure, must report cyber security incidents within six hours of detection.[5] Reportable incidents include ransomware attacks, unauthorized access to IT systems, data breaches, denial of service attacks, and attacks on critical infrastructure. This sixhour reporting window directly applies to industries managing OT environments, requiring robust internal incident detection and escalation capabilities.

c) National Critical Information Infrastructure Protection Centre (NCIIPC)

Established on January 16, 2014 under Section 70A of the IT Act, the National Critical Information Infrastructure Protection Centre (NCIIPC) serves as the national agency for protecting Critical Information Infrastructure (CII).[6]

The NCIIPC is authorized to take measures to reduce vulnerabilities of CII against cyber terrorism, cyber warfare, and other threats. Designated CII sectors include transport, telecommunications, banking, insurance, finance, power, energy, and governance which are precisely the sectors where IT-OT integration is most prevalent and the risks are most acute.

Organizations operating designated CII are required to comply with NCIIPC's guidelines, which address network segmentation, access controls, incident response, and risk assessment for industrial environments. A notable gap is that NCIIPC guidelines are advisory rather than legally binding in all cases, weakening enforcement against non-compliant CII operators. The NCIIPC operates without a publicly transparent enforcement mechanism, making accountability for industrial cybersecurity failures difficult to track judicially.

[4] The information technology (amendment) act 2008, Section 70
[5] Ministry of Electronics and Information Technology (MeitY) and Indian Computer Emergency Response Team (CERT-In) directions under the Information and technology act Section 70B, on 28.04.2022.
[6] Guidelines for protection of critical infrastructure (version 2.0) 2015.

d) National Cyber Security Policy, 2013

The National Cyber Security Policy, 2013 articulates the government's broader objectives of protecting information and infrastructure in cyberspace which calls for establishing capabilities to prevent and respond to cyber threats, minimizing vulnerabilities, and mitigating the impact of cyber incidents through institutional structures, skilled personnel, and collaborative efforts.[7] It aims to build trust and confidence in IT systems and to fortify the regulatory framework for safeguarding the nation's critical information infrastructure, objectives that remain directly relevant to the protection of industrial OT environments integrated with enterprise IT networks.

V. THE DIGITAL PERSONAL DATA PROTECTION ACT OF 2023

India's most significant recent legislative development in the field of data governance is the Digital Personal Data Protection Act, 2023 (DPDP Act) which represents India's first comprehensive data protection law and replaces the earlier Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.[8] The implementing Digital Personal Data Protection Rules, 2025 were notified by the Ministry of Electronics and Information Technology (MeitY), operationalizing the Act's provisions in a phased manner.

• Core Objectives and Scope

The DPDP Act provides for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such data for lawful purposes. It applies to all digital personal data processed within India, and extends to processing of data outside India if it relates to goods or services offered to individuals in India.

This extraterritorial scope is significant for multinational industrial corporations with operations in India that collect and process employee, operational, and customer data across borders.

• Data Fiduciaries and Data Processors in Industrial Contexts

The DPDP Act establishes the concept of "*Data Fiduciaries*" which are the entities that

[7] Ministry of Communication and Information Technology, National Cyber Security Policy of 2013
[8] The Digital Personal Data Protection act of 2023

determine the purpose and means of processing personal data, and "*Data Processors*" that process data on behalf of fiduciaries. In industrial settings, this framework is directly applicable: manufacturing companies, energy utilities, and infrastructure operators that collect personal data of employees, contractors, or end users through digital and OT integrated systems are Data Fiduciaries under the Act. Section 8(1) of the DPDP Act establishes absolute, non transferable liability on Data Fiduciaries for compliance with the Act's provisions, irrespective of any contractual arrangement with a Data Processor.[9] This means that outsourcing data processing, does not dilute the primary organization's legal accountability.

- **Security Obligations and Breach Notification**

Section 8(5) of the DPDP Act mandates that a Data Fiduciary "*shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach*."[10] This obligation is particularly significant for industrial organizations, where personal data may flow across IT and OT systems, remote monitoring platforms, and cloud analytics environments. A breach in any of these interconnected systems can trigger liability under the Act.

Section 8(6) further requires that in the event of a personal data breach, the Data Fiduciary must promptly notify both the Data Protection Board of India and each affected Data Principal.[11] This notification obligation, combined with CERT-In's six hour mandatory reporting window, creates a dual track breach notification mechanism for industrial organizations. Compliance demands that organizations have mature incident detection, triage, and escalation procedures capable of triggering simultaneous notifications to regulatory authorities and affected individuals within extremely compressed timeframes.

- **Significant Data Fiduciaries and Enhanced Industrial Obligations**

The Central Government may designate certain entities as "Significant Data Fiduciaries" (SDFs) based on the volume and sensitivity of data processed, the risk to Data Principals' rights, and the potential impact on national interest. Under the DPDP Rules, 2025, SDFs are subject

[9] The Digital Personal Data Protection act of 2023, Section 8(1)
[10] The Digital Personal Data Protection act of 2023, Section 8(5)
[11] The Digital Personal Data Protection act of 2023, Section 8(6)

to enhanced obligations, including mandatory Data Protection Impact Assessments (DPIAs) and annual independent audits of data processing activities.[12] Large industrial operators managing significant volumes of employee, operational, or consumer data, particularly in sectors such as energy, manufacturing, and telecommunications are likely candidates for SDF designation. Additionally, the DPDP Rules introduce potential data localization requirements for specified sensitive categories, including personal data associated with critical infrastructure, restricting cross border data transfers for such categories.

• **Penalties and Enforcement**

The DPDP Act establishes a penalty structure administered by the Data Protection Board of India. The most significant financial exposure for industrial organizations arises from:

- failure to implement reasonable security safeguards, which attracts penalties of up to ₹250 crore;
- failure to notify the Data Protection Board and affected individuals upon a personal data breach carries penalties of up to ₹200 crore;
- and violations of SDF-specific obligations attract penalties of up to ₹150 crore.[13]

Unlike the percentage of turnover model under the European GDPR, the DPDP Act's fixed maximum penalties make data security an existential fiduciary risk, particularly for smaller and middle sized industrial operators.

• **Relevance to IT-OT Integrated Industrial Environments**

The intersection of the DPDP Act with industrial cyber security is particularly significant in the context of IT-OT convergence. Industrial systems increasingly collect personal data such as biometric access records, employee health monitoring data, vehicle tracking information, and customer usage data in utilities through OT and IIoT systems. Under the DPDP Act, all such data flows are subject to the Act's consent, security, and breach notification requirements. Grant Thornton Bharat has specifically observed that with the release of the DPDP Rules in 2025, manufacturers must implement strict consent based data collection, anonymization of

[12] The Digital Personal Data Protection rules 2025, Ministry of Communication and Information Technology.
[13] The Digital Personal Data Protection act of 2023, Section 33(1) read with The Schedule.

worker and IoT data, and enhanced cyber security across supply chains.[14] Industrial organizations must therefore integrate DPDP Act compliance into their broader OT and security governance frameworks, treating data protection not as a standalone IT compliance matter but as an integral component of industrial risk management.

VI. CONSTITUTIONAL FOUNDATION OF CYBER LAWS IN INDIA

a) Justice K.S. Puttaswamy vs. Union of India (2017)

Justice K.S. Puttaswamy, a retired Karnataka High Court judge, challenged the constitutional validity of the Aadhaar scheme, arguing that mandatory biometric collection violated the right to privacy. The case required settlement of a fundamental question that whether privacy is a fundamental right under the Indian Constitution. In a unanimous, historic decision, the nine-judge bench declared that the Right to Privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution. The Court explicitly overruled previous judgments in M.P. Sharma and Kharak Singh that had held otherwise. Before Puttaswamy, companies could argue that users had no enforceable privacy rights in their data. Post-Puttaswamy, every data breach, every unauthorized data sharing, and every surveillance overreach must be tested against the proportionality doctrine. The Digital Personal Data Protection Act, 2023 (DPDPA) is a direct legislative response to this judgment. [15] The principles that were established in this landmark judgment were that ***Privacy includes bodily integrity, personal autonomy, and informational privacy; The right extends to protection of personal data in the digital age; Any restriction must meet the tests of legality, necessity, and proportionality; Privacy is not absolute but can only be curtailed through just, fair, and reasonable procedure.***

b) Dhule Vikas Sahakari Bank v. AXIS Bank (2025),

The case centered on whether AXIS Bank's failure to implement Two-Factor Authentication (2FA) for high value transactions constituted a breach of "reasonable security practices and procedures" under Section 43A of the IT Act and a violation of RBI cybersecurity guidelines. The Adjudicating Officer ruled in favour of the complainant, awarding Rs. 1.76 crore in

[14] Grant Thornton Bharat, *Demystifying the Digital Personal Data Protection Act, 2023* (2025), https://www.grantthornton.in/services/esg-risk-consulting/cyber/demystifying-the-digital-personal-data-protectionact-2023/.
[15] Analysis by Adv (Dr.) Prashant Mali, Cyber Law Blog India https://www.prashantmali.com/cyber-law-blog-india/important-cyber-law-case-laws-in-india

compensation with 18% compound interest, totaling over Rs. 2.5 crores - establishing that banks must implement security measures proportionate to transactional risk, that absence of 2FA is an independently actionable security failure, that compound interest is awardable to prevent delayed justice from becoming denied justice, that mental agony damages are available in cyber fraud cases. The case also established that ***banks cannot deflect liability onto customers when the fraud is rooted in the bank's own deficient security infrastructure, making this a watershed precedent for banking cyber security adjudications across India***.[16]

c) National Insurance Company Ltd. v. IFFCO Tokio General Insurance Co. Ltd. (2016)

This civil case directly addresses corporate liability for inadequate cybersecurity measures. The plaintiff filed suit against the defendant for a data breach that resulted in the theft of customer data, arguing that inadequate cybersecurity measures had facilitated the violation. The court found IFFCO Tokio negligent and ordered the payment of compensation for the damages suffered. This judgment is significant for two reasons in the industrial cybersecurity context: it establishes that ***civil courts will impose liability on organizations that fail to maintain adequate cybersecurity standards, regardless of whether the breach was perpetrated by an external attacker***; and second, ***it demonstrates that the duty of care in data security applies not merely to IT systems but to any organizational infrastructure through which sensitive data flows including OT-integrated systems in industrial settings***.[17]

d) G. Sundarrajan v. Union of India (2013) 6 SCC 620

This Supreme Court decision, concerning the Kudankulam Nuclear Power Plant, is foundational to understanding India's judicial approach to safety and risk management in critical industrial infrastructure. The Court upheld the commissioning of the plant but imposed a set of safety conditions, emphasizing that industrial operations involving critical infrastructure must be subject to continuous monitoring, emergency preparedness, transparent risk management mechanisms, and independent regulatory oversight. The Court's ***reasoning reflects the principle that technological and industrial development cannot be pursued at the***

[16] Id

[17] National Insurance Co. Ltd. v. IFFCO Tokio General Insurance Co. Ltd., Civil Suit (2016) (India), *discussed in* Rahul Tyagi, *India: Cybersecurity Laws and Regulations 2025*, Int'l Comparative Legal Guides (Nov. 6, 2024), https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india/.

cost of human life and environmental safety, a principle that extends directly to cyber security risk management in industrial environments.[18]

This judicial reasoning was reinforced in light of the 2019 Kudankulam malware incident, wherein a cyber intrusion was detected in the administrative IT network of the plant. Although the nuclear control systems were reportedly isolated, the incident illustrated the real world dangers of IT-OT convergence in critical infrastructure and the imperative for rigorous network segregation, intrusion detection, and incident response capabilities, precisely the operational safeguards the

Court had mandated in the context of physical safety risk management

VII. CONCLUSION

Industrial cyber risk management at the intersection of IT and OT security is no longer merely a technical or operational concern, it is a matter of constitutional obligation, statutory compliance, regulatory duty, and judicial accountability in India. The convergence of IT and OT systems in critical sectors has dramatically expanded the cyber attack surface, with potential consequences ranging from operational disruption to threats to human life and national security.

India's legal and regulatory framework has evolved substantially to address these risks. The IT Act, 2000 provides foundational offences and liability mechanisms. CERT-In's 2022 Directions impose rigorous incident reporting obligations. The NCIIPC provides sector specific guidance for critical infrastructure protection. The landmark Digital Personal Data Protection Act, 2023, operationalized through the DPDP Rules, 2025, introduces a comprehensive regime of data security obligations, breach notification duties, and substantial financial penalties that directly apply to industrial organizations processing personal data through IT-OT integrated systems. The DPDP Act's requirements for reasonable security safeguards, mandatory breach notification, and enhanced obligations for Significant Data Fiduciaries collectively compel industrial organizations to treat data protection as an inseparable component of industrial cyber risk governance.

[18] G. Sundarrajan v. Union of India, (2013) 6 SCC 620 (India).