ujiyari

UPSC & STATE PCS CURRENT AFFAIRS · UJIYARI.COM

DAILY CURRENT AFFAIRS

Shortage of Cybersecurity Talent in India: A Digital Economy Risk

14 March 2026

SUBJECTS COVERED

SCIENCE & TECH | SECURITY & DEFENCE

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator •
linkedin.com/in/epicbharat

Shortage of Cybersecurity Talent in India: A Digital Economy Risk

14 March 2026 · 11 min read ·

On this Page

WHY IN NEWS

Reporting on **11 March 2026** highlighted that India has approximately **3.8 lakh cybersecurity professionals** against a projected demand of **12 lakh by 2027**, as the **Data Security Council of India (DSCI)** and **NASSCOM** flagged a persistent and widening talent gap even as cyber threat detections in India surpassed **265 million incidents** between October 2024 and September 2025 — approximately **505 detections every minute**.

SPEED WITHOUT SECURITY IS FRAGILITY

India's digital transformation is one of the most consequential public infrastructure stories of the past decade. The country now operates **Unified Payments Interface (UPI)** — handling over 16 billion transactions monthly as of early 2026 — along with **Aadhaar** (over 1.4 billion enrollments), **DigiLocker**, **CoWIN**, **GSTN**, **GeM (Government e-Marketplace)**, and an expanding stack of Digital Public Infrastructure (DPI) that delivers government services at scale. The financial sector, telecommunications, healthcare, and defence procurement all run on interconnected digital systems.

Every expansion of this digital stack enlarges what security professionals call the **attack surface** — the total set of points through which an adversary can attempt to enter, disrupt, or extract data from a system. A country that digitises at India's pace without a commensurate investment in cybersecurity capacity is not only creating efficiency; it is creating systemic vulnerability. The cybersecurity talent shortage is not a human resources problem. It is a national infrastructure problem.

THE SCALE OF THE GAP

The numbers are precise and alarming. According to estimates reported in March 2026 by industry bodies including **NASSCOM** and **DSCI (Data Security Council of India)**, India currently employs approximately **3.8 lakh (380,000) cybersecurity professionals**. Projected demand could reach **12 lakh (1.2 million) by 2027** — implying a gap of over **8 lakh positions** within a two-year horizon.

Globally, the cybersecurity talent shortage is estimated at approximately **4.8 million professionals** by **ISC² (International Information System Security Certification Consortium)** in its 2024 Workforce Study — a 19% year-on-year increase and the largest recorded figure. The global cybersecurity workforce has stalled at an estimated **5.5 million people**, marking a significant slowdown from the 8.7% growth recorded in 2023. India's share of this global gap is significant and growing. The shortfall is particularly severe in specialised roles: cloud-security engineering, operational technology (OT) and industrial-control system (ICS) security, threat intelligence, AI-assisted threat detection, digital forensics, and security architecture.

Industry data from 2025-26 also points to a **30–40% shortfall** in niche cyber roles specifically, with hiring cycles for qualified security analysts and engineers exceeding **90 days** on average — a critical delay in a domain where speed of response determines the outcome of incidents. The offer-acceptance ratio for qualified cybersecurity candidates stands at approximately **70%**, reflecting a seller's market where skilled professionals can be highly selective.

THE THREAT LANDSCAPE: WHY DELAY IS DANGEROUS

The talent gap is not merely an academic concern about future workforce planning. It is a present operational deficiency occurring while threats escalate.

Reporting from **Seqrite** (Quick Heal Technologies' enterprise arm) and other threat intelligence sources for the period October 2024 to September 2025 showed approximately **265.52 million cyber threat detections in India** — equivalent to approximately **505 detections every minute**. Spyware detections increased by **273% in the first half of 2025** compared to the preceding year. Password-stealing malware incidents in 2025 numbered approximately **111,281**, an increase of nearly **17.9%**. Ransomware attacks on Indian organisations — including hospitals, government departments, and manufacturing firms — increased in both frequency and sophistication.

The financial sector has been a priority target: RBI's 2025 annual report on cyber incidents noted a sharp rise in attempted intrusions into banking and payment infrastructure. The healthcare sector, particularly after the digitisation of hospital management systems under **Ayushman Bharat Digital Mission (ABDM)**, has become an increasingly targeted vertical because medical records command high value on dark web markets.

The convergence of an expanding attack surface with a depleted defender workforce creates the conditions for high-impact incidents that India's current cyber capacity may be unable to contain.

INDIA'S INSTITUTIONAL ARCHITECTURE: STRENGTHS AND GAPS

India has built a substantial institutional framework for cybersecurity over two decades, though significant gaps remain.

The IT Act and CERT-In

The **Information Technology Act, 2000** — amended significantly in 2008 — is the foundational legislation for cybercrime and digital governance in India. It establishes the legal framework for electronic records, digital signatures, cybercrime offences, and network security obligations. Under the IT Act, **CERT-In (Indian Computer Emergency Response Team)**, established in **January 2004** under the **Ministry of Electronics and Information Technology (MeitY)**, functions as the national nodal agency for cybersecurity incident response, coordination, and advisories.

CERT-In operates a 24x7 incident response mechanism and publishes advisories on vulnerabilities, malware, and phishing campaigns. In April 2022, MeitY issued **mandatory cybersecurity directions** under Section 70B of the IT Act, requiring organisations to report cyber incidents to CERT-In within **6 hours** — one of the strictest reporting timelines in any jurisdiction globally.

NCIIPC and Critical Infrastructure Protection

The **National Critical Information Infrastructure Protection Centre (NCIIPC)**, established in January 2014 under the IT Act and operating under the **National Technical Research Organisation (NTRO)**, is designated as the national nodal agency for protecting India's **Critical Information Infrastructure (CII)**. NCIIPC works with sectors designated as critical — power, banking, telecom, transport, e-governance, and strategic enterprises — to establish sector-specific security standards and coordinate incident response.

National Cyber Security Policy 2013 and Its Unfinished Successor

The **National Cyber Security Policy (NCSP) 2013**, released in July 2013, was India's first comprehensive policy document for cybersecurity. It set targets including creating a workforce of **500,000 cybersecurity professionals by 2018** — a target that was not met. It also proposed establishing a National Cyber Coordination Centre (NCCC), which CERT-In has since made operational.

A **revised National Cyber Security Policy** — sometimes referred to as NCSP 2020 — was in draft for several years but has not been formally released as of March 2026. This policy vacuum is significant: the 2013 policy predates smartphones at scale, cloud computing's dominance, the rise of DPI, the expansion of IoT devices, and the emergence of AI-enabled attacks. India is operating its most complex digital infrastructure against a 13-year-old policy framework.

Digital Personal Data Protection Act, 2023

The **Digital Personal Data Protection (DPDP) Act, 2023**, passed in August 2023 under MeitY, establishes obligations for **Data Fiduciaries** (organisations that collect and process personal data) to implement appropriate technical and organisational measures to secure personal data. It creates a **Data Protection Board of India (DPBI)** for adjudication. The DPDP Act adds a compliance dimension to cybersecurity — organisations must now prove technical security adequacy, creating demand for cybersecurity professionals in data-protection and governance roles.

WHY THE TALENT PIPELINE IS BROKEN

Curriculum That Does Not Match the Threat

Most Indian engineering colleges teach cybersecurity as a theoretical elective, typically in the final year of a computer science or information technology degree. The curriculum rarely includes live vulnerability labs, capture-the-flag (CTF) exercises, security operations centre (SOC) simulations, red team/blue team exercises, or forensic investigation on real malware samples. Students graduate with theoretical knowledge but no practical skill in the tools — **Wireshark, Metasploit, Splunk, CrowdStrike Falcon, OpenVAS** — that the industry uses daily.

The Certification Barrier

Industry-recognised cybersecurity certifications — including **CISSP (Certified Information Systems Security Professional)**, **CEH (Certified Ethical Hacker)**, **CompTIA Security+**, and **OSCP (Offensive Security Certified Professional)** — are expensive, costing between Rs 30,000 and Rs 2 lakh per certification, and are often inaccessible for students from non-metropolitan institutions. While platforms like **CDAC (Centre for Development of Advanced Computing)** and **NASSCOM FutureSkills Prime** offer some accessible programmes, scale remains limited.

The Experience Paradox

Employers demand 2–3 years of hands-on experience for even mid-level security analyst roles. But entry-level roles with mentored on-the-job training are rare. The result is that thousands of interested graduates cannot enter the profession, while vacancies for experienced professionals go unfilled. Breaking this paradox requires apprenticeship models, structured internships, and tiered entry pathways linked to practical skill assessments rather than just certifications.

Outsourcing as a Workaround and Its Limits

Industry data indicates that approximately **92% of Indian organisations** rely on outsourced or managed security services in some form. Managed Security Service Providers (MSSPs) and Security Operations Centre-as-a-Service (SOCaaS) offerings have grown rapidly. Outsourcing is a legitimate strategy for SMEs and even large enterprises for routine monitoring and compliance.

However, outsourcing has a structural limitation: **strategic cyber capability cannot be permanently outsourced**. Critical government infrastructure, defence networks, financial market infrastructure, and public digital platforms require in-house security teams with clearances, institutional knowledge, and continuity. India cannot outsource the defence of Aadhaar, GSTN, UPI, or its power grid to a third party. National cyber sovereignty requires domestic talent at scale.

WHAT INDIA MUST BUILD

India needs a layered, long-term response structured across four dimensions.

At the education level, the **All India Council for Technical Education (AICTE)** and the **University Grants Commission (UGC)** must mandate practical cybersecurity curriculum reforms — mandatory SOC labs, ethical hacking exercises, and cloud-security practicals — across all computer science and IT programmes. The **IITs, NITs, and IIITs** should develop specialised postgraduate and doctoral programmes in cybersecurity, information assurance, and digital forensics.

At the skilling level, **NASSCOM FutureSkills Prime**, **CDAC**, and **NIC (National Informatics Centre)** should massively expand subsidised, practically-oriented cybersecurity training with clear pathways to employment. Apprenticeship frameworks under the **National Apprenticeship Promotion Scheme (NAPS)** should be extended specifically to cybersecurity roles.

At the policy level, a revised and comprehensive **National Cyber Security Policy** must be released, incorporating the realities of AI-enabled threats, cloud-native infrastructure, DPI security, OT/ICS security, and the DPDP Act's compliance requirements. A clear national **cybersecurity workforce development strategy** — with specific targets, timelines, and institutional responsibilities — must accompany it.

At the research level, India must fund dedicated cybersecurity research centres that work on threat intelligence, vulnerability discovery, and indigenous security tools — reducing dependence on foreign security software for critical applications.

UPSC RELEVANCE

IT Act 2000, CERT-In (est. 2004), NCIIPC, NTRO, National Cyber Security Policy 2013, DPDP Act 2023, NASSCOM, DSCI, CDAC, NIC, AICTE, ISC², CISSP, Digital Public Infrastructure (DPI), UPI, Aadhaar, ABDM.

MAINS GS-3:

Cybersecurity, critical information infrastructure protection, digital economy, skilling for digital India, technology governance.

INTERVIEW:

Is India's pace of digital expansion ahead of its security capability? How should India approach digital sovereignty?

📌 FACTS CORNER — KNOWLEDGEPEDIA

INDIA'S CYBERSECURITY WORKFORCE GAP:

Current cybersecurity professionals in India: Approximately **3.8 lakh (380,000)**

Projected demand by 2027: Approximately **12 lakh (1.2 million)**

Gap: Over **8 lakh positions**

Global cybersecurity shortage (ISC² 2024 Workforce Study): Approximately **4.8 million professionals** (19% YoY increase)

Global cybersecurity workforce size: Approximately **5.5 million** (0.1% YoY growth — stalled)

Shortfall in niche cyber roles: 30–40%

Average hiring cycle for specialised cyber roles: Over **90 days**

Offer acceptance ratio: Approximately **70%**

Organisations using outsourcing for cyber support: Approximately **92%**

THREAT LANDSCAPE DATA (INDIA):

Total threat detections (Oct 2024–Sep 2025): Approximately **265.52 million** (source: Seqrite)

Detections per minute: Approximately **505**

Spyware increase (H1 2025 vs H1 2024): 273%

Password-stealer incidents (2025): Approximately **111,281** — up **17.9%** year-on-year

INSTITUTIONAL ARCHITECTURE:

Information Technology (IT) Act: 2000 (amended 2008) — foundational cybersecurity legislation

CERT-In: Indian Computer Emergency Response Team — established **January 2004** under MeitY; national nodal agency for incident response

Mandatory incident reporting: Within **6 hours** of discovery (CERT-In directions, April 2022)

NCIIPC: National Critical Information Infrastructure Protection Centre — established **January 2014**; under NTRO; protects Critical Information Infrastructure (CII)

NTRO: National Technical Research Organisation — intelligence organisation under PMO; parent of NCIIPC

National Cyber Security Policy (NCSP): Published **July 2013** — target of 500,000 cyber professionals by 2018 (not met); draft NCSP 2020 not yet released as of March 2026

DPDP Act: Digital Personal Data Protection Act, **August 2023** — mandates technical security for data fiduciaries; establishes Data Protection Board of India (DPBI)

Cyber Swachhta Kendra: Botnet Cleaning and Malware Analysis Centre under CERT-In

KEY TRAINING AND SKILLING BODIES:

NASSCOM: National Association of Software and Service Companies — industry body; runs FutureSkills Prime platform

DSCI: Data Security Council of India — NASSCOM subsidiary; produces cybersecurity reports and standards

CDAC: Centre for Development of Advanced Computing — government body; offers cybersecurity training programmes

NIC: National Informatics Centre — government IT agency under MeitY; manages e-governance infrastructure

AICTE: All India Council for Technical Education — regulates technical education; responsible for curriculum standards

KEY CERTIFICATIONS (INDUSTRY-RECOGNISED):

CISSP: Certified Information Systems Security Professional (ISC²)

CEH: Certified Ethical Hacker (EC-Council)

CompTIA Security+: Entry-level cybersecurity certification

OSCP: Offensive Security Certified Professional — highly practical, widely respected for penetration testing

DIGITAL PUBLIC INFRASTRUCTURE AT RISK:

UPI: Over 16 billion transactions/month (early 2026) — critical payment infrastructure

Aadhaar: Over 1.4 billion enrollments — identity backbone

GSTN: Goods and Services Tax Network — tax infrastructure

ABDM: Ayushman Bharat Digital Mission — digital health records; high-value target

OTHER RELEVANT FACTS:

Cybersecurity covers **cloud security, digital forensics, OT/ICS security, SOC operations, threat intelligence, identity and access management** — not just "stopping hackers"

The NCSP 2013 predates **smartphones at scale, cloud dominance, DPI, IoT proliferation, and AI-enabled attacks**

India cannot outsource defence of its critical public digital platforms — national cyber sovereignty requires domestic talent

Cyber capacity is a component of **digital sovereignty** and **national security**, not only IT workforce planning

Sources: CERT-In, MeitY, Data Security Council of India, NASSCOM, Seqrite, The Economic Times

RELATED EDITORIALS

THE HINDU
Fire and Fury — The Ill-Conceived War on Iran and Its Global Fallout
20 Mar

INDIAN EXPRESS
Energy Security Under Threat — The Ras Laffan Attack and India's Vulnerabilities
20 Mar

THE HINDU
AI-Powered Taxation — Project Insight's Gains and Governance Risks
20 Mar

HINDUSTAN TIMES
Drones and the Future of War — India's Defence Manufacturing Imperative
20 Mar

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

📖 **Read Full Article on Ujiyari →**

https://ujiyari.com/daily/2026/03/14/cybersecurity-talent-shortage-india/