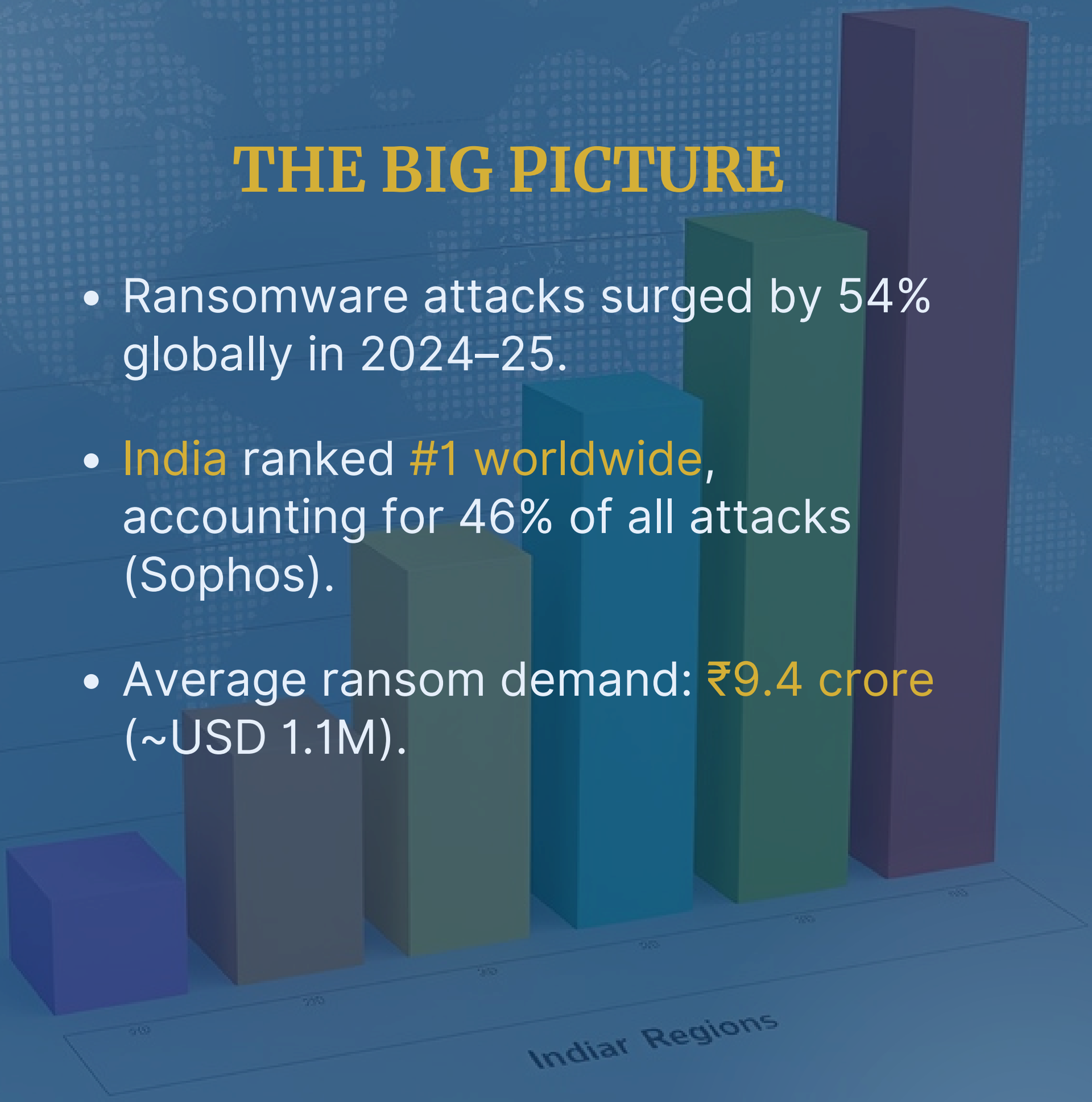
DO YOU KNOW?

INDIA SAW HALF OF ALL GLOBAL RANSOMWARE ATTACKS

What went wrong, and what can we do next?

THE BIG PICTURE

- Ransomware attacks surged by 54% globally in 2024–25.
- India ranked #1 worldwide, accounting for 46% of all attacks (Sophos).
- Average ransom demand: ₹9.4 crore (~USD 1.1M).



WHY INDIA?

- Rapid digital transformation in Small and Medium Enterprises (SMEs) without matching cybersecurity maturity.
- Heavy reliance on cloud & third-party IT services.
- Low reporting rates, high payment frequency.

THE RISE OF CYBERCRIME AS A SUBSCRIPTION MODEL

- Ransomware-as-a-Service (RaaS) lets criminals “rent” attack kits and profit-share with developers.
- Most active RaaS groups in India: LockBit, BlackCat/ALPHV, and Akira.
- Increasing use of AI-generated phishing & credential harvesting.

THE HUMAN FACTOR

- 76% of Indian ransomware incidents start with phishing or credential theft*.
- Remote workforces and hybrid setups remain primary weak links.

* THE STATE OF RANSOMWARE IN INDIA 2025 by SOPHOS

IMPACT SNAPSHOT

- Average downtime: 9.2 days (up from 6.5).
- Data encrypted: 73% of incidents.
- Ransom paid: 64% of victims among the highest globally.
- Recovery cost (incl. downtime): ₹13.2 crore average.

CERT-IN FINDINGS: (2024 REPORT)

- Ransomware attacks concentrated in:
  - IT/ITeS (27%)
  - Manufacturing (21%)
  - Healthcare (14%)
- Surge in “double extortion” tactics: encryption + data leak threats.

LEGAL AND GOVERNANCE IMPLICATIONS

- IT Act 2000 (Sections 43 & 66): Covers unauthorised access, data theft.
- CERT-In Directions 2022: 6-hour breach reporting requirement.
- DPDP Act 2023: Data fiduciaries liable for breach prevention.

India lacks a dedicated ransomware reporting law or victim support mechanism.

PREVENTION & PREPAREDNESS

What businesses should do now:

✅ Enforce multi-layered backups (offline + encrypted).

✅ Conduct phishing simulations & employee training.

✅ Maintain updated patch management & MFA.

✅ Prepare legal + technical incident response playbooks.

✅ Partner with CERT-In–empanelled audit agencies.

Centre for Research and
Governance on Cyber Law

Empower Yourself—
Know Your Digital Rights!

Share this post to spread awareness.
Follow CRGCL for more updates on digital governance and cyber law.

www.crgcl.com