Issue #19, April 2026

IMGC
Defining Tomorrow

THE TECH TALK

Beyond Defense: Recovery as the True Test of Cyber Readiness

Organizations are being outpaced by today's cyber threat landscape. As cloud complexity grows, upstream and downstream partners become frequent entry points, and nearly a third of incidents now originate outside the enterprise perimeter. Even strong security programs can be disrupted. The rapid adoption of automation and AI has further shortened attack cycles, leaving traditional defense models struggling to keep up.

By 2026, true cyber strength is defined less by flawless prevention and more by the ability to restore operations swiftly and with certainty. Regulators and insurers increasingly expect evidence of reliable recovery, uncompromised system rebuilds, and safeguarded data. For business leaders, resilience has become a core requirement—critical to business continuity and essential for preserving confidence in a volatile digital environment.

Supply Chain: Cybersecurity's Open Door

Expanding AI-Powered Attack Surface

- By 2026, many organizations are projected to operate more self-directing AI agents than human users
- **88% of organizations have already experienced AI-related security incidents**
- Once compromised, AI agents can rapidly move data out of environments, elevate access rights, or make high-impact changes to cloud settings
- Limitations in current AI platforms reduce visibility into agent-to-agent interactions, opening new and largely unmonitored paths for attackers

Cloud Security Risk Snapshot

- **Misconfigurations cause 32% of global cloud security incidents** and are expected to drive **90% of cloud failures by 2026**
- **80% of companies** experienced at least one cloud breach in the past year due to insecure APIs, identity drift, and shadow APIs
- **78% of organizations use hybrid or multi-cloud setups,** creating visibility gaps and increasing risk
- **Human error accounts for 68% of cloud outages,** highlighting operational weaknesses

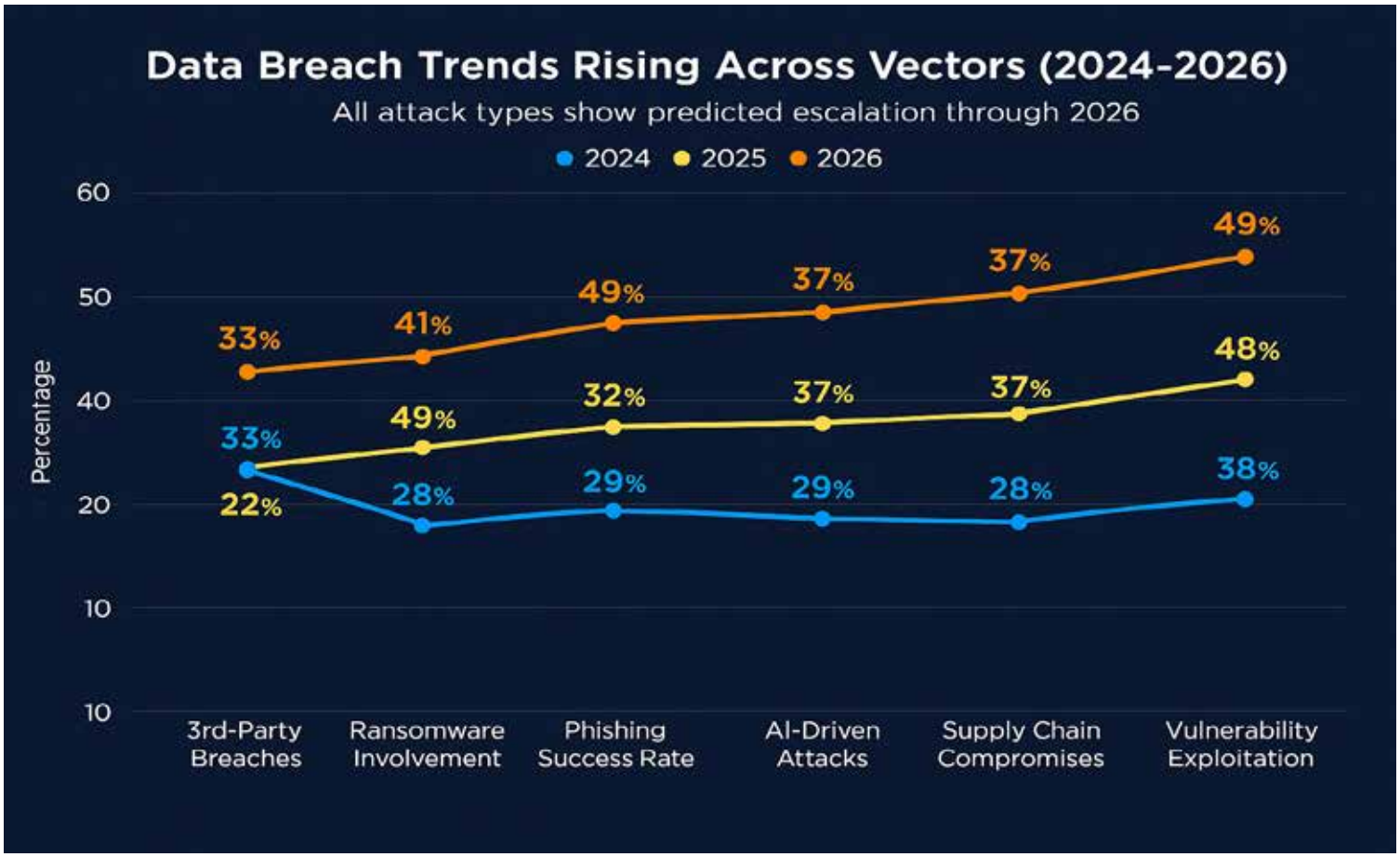
The Growing Weight of Global Regulation on Compliance

Regulatory Change: What Leaders Must Know Data Protection and Operational Resilience (India DPDPA | EU DORA & NIS2)

- India's DPDPA tightens control over how personal data is collected, used, and retained, with strict consent and purpose-limitation requirements. Organizations must prove disciplined data practices, minimal collection, lawful processing, and the ability to erase data on demand.
- Cross-border data movement is increasingly restricted, requiring alignment with approved jurisdictions and enhanced safeguards. By 2026, compliance is no longer procedural; it is a core business responsibility with reputational and financial consequences. EU DORA and NIS2 raise the bar on encryption, key governance, incident response, and resilience testing.
- The EU AI Act, fully enforced from August 2026, adds another layer of complexity for global operations navigating inconsistent regulatory models
- Regulatory fragmentation increases the likelihood of configuration gaps, audit failures, and significant penalties

Rising Bar for Cyber Resilience

- Organizations are now expected to demonstrate proven, repeatable recovery, not just documented plans
- Regulators and insurers increasingly look for evidence of secure rebuild capabilities and verified system integrity after incidents
- Enterprises that invest in strong identity controls and cleanroom recovery benefit from:
  i. Faster cyber-insurance approvals
  ii. Greater regulator confidence and reduced scrutiny



Cybersecurity Reframed: Resilience, Speed, and Certainty

- Cyber risk is accelerating as digital ecosystems expand, supply-chain attacks have doubled, and ~30% of breaches now originate with third parties
- Cloud complexity remains a primary exposure driver, with misconfigurations, hybrid/multi-cloud sprawl, and weak vendor controls fueling incidents
- Automation and AI are increasing attack speed and scale, outpacing traditional security response models
- Regulators and insurers now require provable recovery capabilities, including clean system rebuilds and protected data, before granting approvals or coverage
- Cybersecurity effectiveness is no longer defined by prevention alone the decisive metric is the ability to recover fast, cleanly, and with confidence restoring cleanly, and resuming operations with confidence

"As threats evolve, strong cybersecurity is no longer discretionary; it underpins long-term business stability"

Our Vision:

"Act as a catalyst to make housing affordable in India by enabling risk optimization through data technology leverage"

Our Mision:

- Partner with the housing finance industry to drive financial inclusion goals and promote responsible lending
- Maximise shareholder value while maintaining prudent risk discipline

PROVIDED GUARANTEES IN OVER 400 LOCATIONS
to customers across India

HELPED OVER 1,50,000 FAMILIES
realise their dream of owning a home

For more information scan the QR or visit us at: www.imgc.com

Connect with us:
Send "MG" at +91-73033 88455 on WhatsApp