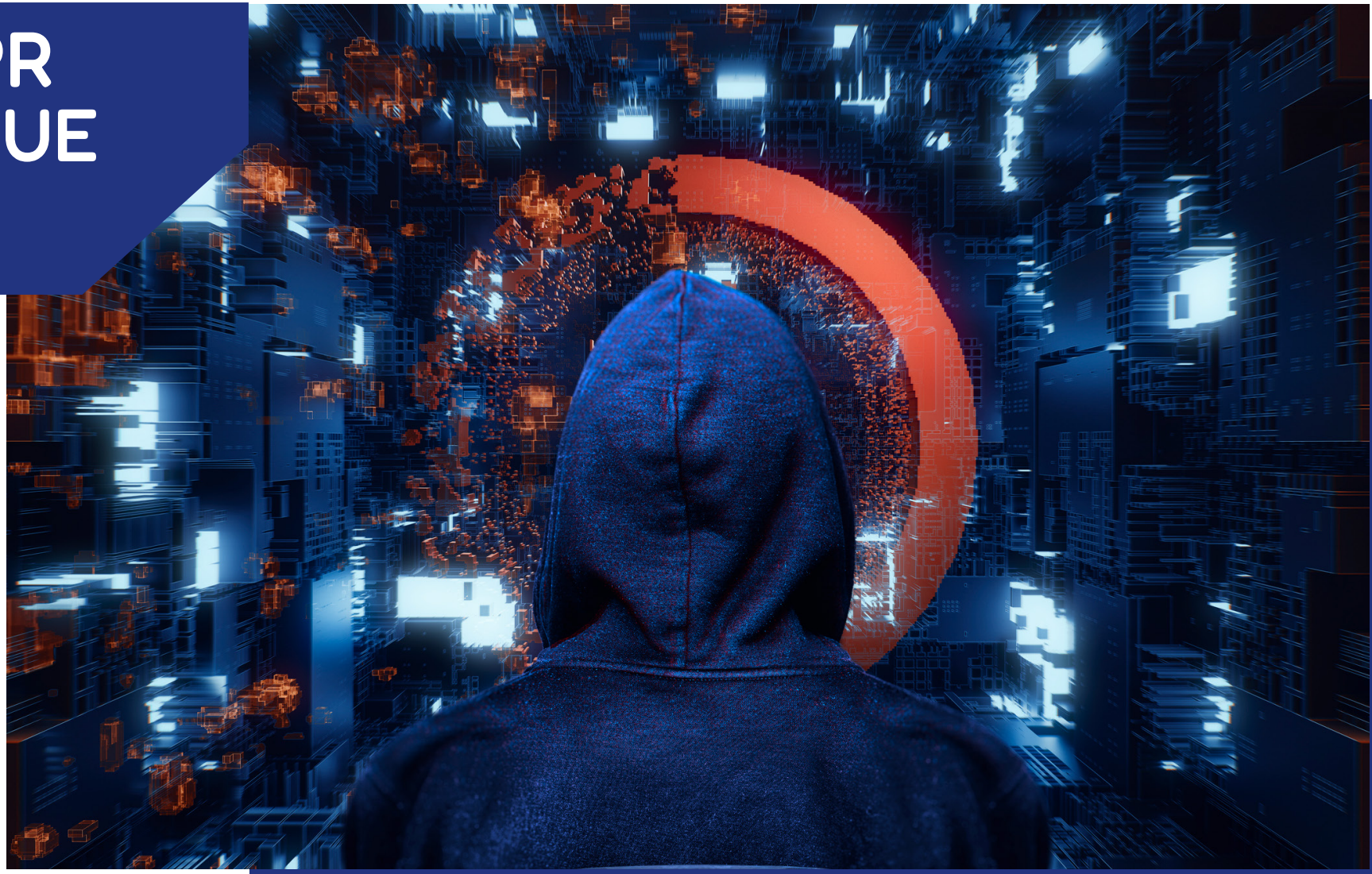
EDME CYBER PLUGG IN MONTHLY NEWSLETTER

APR 2026

APR ISSUE 14



Welcome to the latest edition of our Cyber Insights Newsletter, your comprehensive guide to staying informed about the ever-evolving world of cyber threats, trends, and insurance. As your trusted cyber insurance partner, we bring you curated updates on domestic and international developments, helping you mitigate risks and enhance resilience.

EMERGING TRENDS IN THE CYBER WORLD

The Weaponization of "Agentic" AI:

The shift from static phishing to "Agentic AI" campaigns has accelerated. Unlike traditional scams, these autonomous AI agents engage in real-time, multi-turn conversations with employees, adapting persuasion tactics based on responses to bypass behavioral filters.

Deepfake Identity Fraud Dominance:

According to the Thales 2026 Data Threat Report, 65% of Indian organizations have experienced deepfake-driven incidents. AI-enabled deepfakes are now the primary tool for identity-based attacks, with 64% of Indian firms ranking AI-enabled attacks as their top security risk.

AI-Powered Deepfake Social Engineering:

The proliferation of generative AI tools has enabled threat actors to craft hyper-realistic audio and video deepfakes targeting C-suite executives. In early 2026, multiple financial institutions reported Business Email Compromise (BEC) attacks where AI-cloned voice calls impersonated CFOs to authorize fraudulent wire transfers, marking a significant evolution beyond traditional phishing.

Quantum Computing Threats to Cryptographic Infrastructure:

NIST's finalization of post-quantum cryptographic (PQC) standards in late 2024 accelerated enterprise migration timelines. However, nation-state actors are increasingly employing "harvest now, decrypt later" strategies, intercepting and storing encrypted data today with intent to decrypt once quantum capabilities mature, posing long-term risks to sensitive financial and government communications.

Critical Infrastructure Targeting via OT/ICS Vulnerabilities:

A surge in attacks against Operational Technology (OT) and Industrial Control Systems (ICS) was observed in Q1 2026, with threat actors exploiting unpatched legacy SCADA systems in the energy and utilities sector. CERT-In issued advisories urging asset owners to implement network segmentation and real-time anomaly detection to mitigate cascading disruptions to essential services.

CYBER NEWS

RBI Thwarts 61 Million Cyberattack Attempts in Q3 FY26

The Reserve Bank of India (RBI) reported that its infrastructure successfully repelled over 61 million cyberattack attempts during the October–December 2025 quarter. This represents a significant escalation from 31 million in the previous quarter. The central bank highlighted that no security breaches were reported, attributing the resilience to the integration of advanced AI monitoring systems that detect unusual traffic patterns and vulnerabilities in real-time.

READ MORE >

Mandatory WhatsApp SIM Binding for Indian Users Starts March 1

In an effort to curb rising digital fraud, the Department of Telecommunications (DoT) has enforced "SIM Binding" rules for WhatsApp users in India effective March 1, 2026. The new mandate requires the app to remain continuously linked to the physical SIM card in the primary device, with automated checks occurring roughly every six hours. This move aims to prevent scammers from operating Indian accounts remotely from international locations.

READ MORE >

India Implements Major Ban on Hikvision and TP-Link CCTV Devices

The Government of India has issued a directive restricting the sale and use of foreign surveillance hardware, specifically targeting brands like Hikvision, Dahua, and TP-Link, effective from April 1, 2026. The March announcement focuses on national security concerns regarding foreign chipsets and data exfiltration. This regulatory shift has accelerated the "Make in India" surveillance market, with local brands like CP Plus and Qubo seeing a surge in adoption.

READ MORE >

CERT-In and SIA-India Release Space Cyber Security Guidelines

To protect the country's growing space ecosystem, CERT-In, in collaboration with the SatCom Industry Association (SIA-India), released a comprehensive "Space Cyber Security Framework" in March 2026. The guidelines are designed to secure satellite communications and ground stations against high-level state-sponsored threats, emphasizing the need for end-to-end encryption and supply chain integrity for space-bound assets.

READ MORE >

Government Blocks Developer Platform Supabase Under Section 69A

In a move that impacted thousands of Indian tech startups, the government blocked access to the popular developer database platform Supabase (Postgres Database Platform) in March 2026. While the specific reason for the block under the Information Technology Act was not immediately disclosed, the incident has highlighted the "Shadow IT" risks and the sensitivity of offshore data storage for Indian enterprises.

READ MORE >

CYBER NEWS

Massive "Wiper" Attack Cripples Stryker Global Operations

Medical technology giant Stryker Corporation is reeling from a massive, coordinated cyber attack that has reportedly bricked over 200,000 global endpoints and deleted 50 terabytes of data. The assault, launched shortly after midnight on March 11, 2026, bypassed traditional defenses and likely weaponized the company's own administrative tools to trigger a global reset or "wipe" of its hardware.

READ MORE >

Cegedim Sante Breach Exposes 15.8 Million French Patient Records

In one of the largest healthcare data breaches in European history, attackers infiltrated Cegedim's MonLogicielMedical platform, used by 3,800 French doctors, in late 2025 but the breach was only publicly confirmed on March 3, 2026, four months after detection. The stolen dataset included 15.8 million patient records, with 165,000 files containing highly sensitive free-text clinical notes detailing HIV status, psychiatric diagnoses, sexual orientation, and mental health conditions. The prolonged silence drew sharp regulatory scrutiny over breach disclosure timelines.

READ MORE >

AstraZeneca Hit by LAPSUS$ Ransomware; Source Code and Cloud Credentials Compromised

Global pharmaceutical giant AstraZeneca was targeted by the LAPSUS$ ransomware group in March 2026, resulting in the exfiltration of approximately 3GB of highly sensitive data. The stolen payload included proprietary source code, cloud infrastructure configurations across AWS, Azure, and Terraform, as well as private keys and vault credentials. The incident raised serious concerns about third-party access governance and secrets management within large-scale pharmaceutical environments.

READ MORE >

EvilTokens OAuth Phishing Campaign Enables Mass Microsoft 365 Account Takeovers

In March 2026, ANY.RUN analysts detected a sharp surge in "EvilTokens," a sophisticated phishing campaign exploiting Microsoft's OAuth Device Code flow, with over 180 malicious URLs identified within a single week. Unlike traditional credential -harvesting attacks, EvilTokens bypassed MFA entirely by tricking users into entering verification codes on the legitimate Microsoft portal, causing Microsoft to issue OAuth tokens directly to the attacker. The campaign impacted organizations across government, finance, healthcare, and technology sectors globally, marking a fundamental shift from password theft to token-based account takeover.

READ MORE >

Stats South Africa Ransomware Attack Disrupts National Data Infrastructure

Statistics South Africa, the country's official national statistics agency, confirmed a ransomware attack in March 2026 involving both large-scale data exfiltration and active ransom demands. Attackers claimed access to sensitive national datasets, raising concerns over data integrity and public trust in government statistical systems.
The dual-objective attack financial extortion combined with reputational disruption reflects a growing trend of ransomware groups targeting public sector bodies to maximize societal impact.

READ MORE >

01
CASE STUDY

Brief Summary:

A mid-sized healthcare diagnostics provider operating a network of laboratories across South India experienced a coordinated ransomware attack that encrypted its primary patient management system and backup servers. The incident resulted in a total operational shutdown for four days, forcing the manual processing of reports and the rescheduling of over 5,000 appointments. Attackers demanded a ransom of 15 BTC (approximately ₹9 crore) for the decryption key and threatened to leak 250GB of sensitive patient data on a dark web forum.

Root Cause Analysis:

Unpatched Legacy VPN:
The initial point of entry was an unpatched vulnerability in a legacy VPN gateway that had been slated for decommissioning but remained active without Multi-factor Authentication (MFA).

Lack of Network Segmentation:
Once inside, the threat actors moved laterally across the flat network architecture, gaining administrative access to the central database and the off-site backup repository which was incorrectly mapped as a local drive.

Inadequate Backup Strategy:
The organization relied on 'hot' backups that were connected to the network, allowing the ransomware to encrypt the recovery files simultaneously with the production data.

Loss and Insurance Applicability:

- The total financial impact was estimated at ₹3.2 crore, including business interruption losses, forensic investigator fees, and data restoration costs.
- The firm opted not to pay the ransom and instead performed a manual restoration from an older, physical offline backup.
- Insurance Applicability: The claim was partially accepted. The insurer covered forensic costs and data restoration. However, a 30% "co-insurance" penalty was applied to the business interruption payout because the organization had failed to implement MFA on all remote access points as declared in their original insurance proposal.

Recommended Post-Incident Measures:

Endpoint Detection and Response (EDR): Deploy EDR tools across all servers and workstations to provide real-time visibility and automated containment of suspicious processes.

Immutable Backups: Implement an "Air-Gapped" or immutable cloud backup solution that prevents data from being deleted or encrypted, even with administrative credentials.

Vulnerability Management: Establish a strict 14-day patching cycle for all "Critical" and "High" rated vulnerabilities on internet-facing assets.

02
CASE STUDY

Brief Summary

A leading regional logistics and supply chain firm specializing in cold-storage transport suffered a significant data breach involving its proprietary routing and client database. A third-party developer inadvertently committed an API secret key to a public GitHub repository during a routine software update. Within 48 hours, threat actors utilized the key to bypass the company's cloud firewall and exfiltrate records pertaining to 45 corporate clients and 12,000 delivery personnel.

Root Cause Analysis:

Secret Management Failure:
The organization lacked an automated secrets management tool, leading to the hard-coding of API credentials within the application source code.

Shadow IT/Development Gaps:
The breach occurred in a "testing" environment that was connected to live production data but did not have the same level of security monitoring or audit logging.

Public Repository Exposure:
There was no automated scanning of public repositories to alert the security team when corporate assets or credentials were leaked externally.

Loss and Insurance Applicability:

- The breach resulted in a ₹1.5 crore loss, primarily driven by regulatory notification requirements, legal counsel for GDPR/DPDP compliance, and a "reputation management" campaign to retain key corporate accounts.
- The company also faced a potential fine from local regulators regarding the exposure of PII (Personally Identifiable Information).
- Insurance Applicability: The claim was accepted in full under the 'Privacy Liability' and 'Data Breach Response' sections of the policy. The insurer facilitated the appointment of a specialist "Breach Coach" and covered the cost of credit monitoring for the impacted delivery personnel.

Recommended Post-Incident Measures:

Secret Scanning Tools: Integrate automated tools into the CI/CD pipeline to scan code for secrets, keys, and tokens before they are pushed to any repository.

Database Masking: Implement data masking and tokenization in non-production environments to ensure that even if a test environment is breached, no sensitive PII is exposed.

API Security Audit: Conduct a comprehensive audit of all external-facing APIs to ensure they utilize OAuth 2.0 and have strict rate-limiting and IP-whitelisting enforced.

DATA SPOTLIGHT

The Deepfake Surge & The Crisis of Algorithmic Trust

Supporting Statistics:

- **Deepfake Fraud Velocity:** Deepfake-related fraud attempts have surged by 2,137% over the last three years. In March 2026, live video and voice manipulation incidents targeting C-suite executives rose to 41% year-over -year, marking a shift from static image manipulation to real-time synthetic impersonation.
- **The "Human Detection" Failure:** Human detection rates for high-quality video deepfakes have plummeted to 24.5%. Furthermore, AI-generated phishing campaigns now achieve a 54% click-through rate, compared to just 12% for manually crafted lures, as LLMs successfully mimic internal organizational tone and context.
- **Machine Identity Overload:** For the first time, non-human identities (service accounts, bots, and AI agents) outnumber human users by a ratio of 45:1 in enterprise environments. 51% of developers now cite unauthorized or excessive API calls from autonomous AI agents as a primary security concern.
- **The Post-Quantum Countdown:** With Gartner predicting that current asymmetric cryptography (RSA/ECC) will be rendered unsafe by 2030, "Harvest Now, Decrypt Later" (HNDL) attacks have increased. Organizations have a narrowing four-year window to implement post-quantum cryptographic (PQC) agility before historical data captures become exploitable.
- **India's Regulatory Enforcement Peak:** Following the full operationalization of the DPDP Act and SEBI's CSCRF, Indian financial entities have seen a 35% increase in cross-border data audits. Non-compliance with the 6-hour reporting mandate has triggered the first wave of formal regulatory inquiries for major domestic infrastructure providers.

Implications and Tactical Risks:

- **Agentic Identity Hijacking:** As organizations deploy autonomous AI agents for workflows, these agents are becoming distinct digital actors with high levels of privilege. The risk of "Agentic Privilege Creep" necessitates a transition from static IAM to dynamic, task-specific, and Just-In-Time (JIT) access for all non-human entities.
- **The Erosion of Biometric Trust:** Traditional biometric verification (facial and voice recognition) is no longer a sufficient standalone "proof of life." Enterprises must adopt Multi-Modal Identity Verification that combines biometrics with hardware-backed keys and behavioral telemetry to counter synthetic media.
- **Sovereign API Risk:** APIs are no longer just technical endpoints; they are board-level assets governing the scale and risk of the entire platform. A single "authorization drift" in a third-party SaaS integration can now cascade through an entire supply chain in under 15 minutes.

VULNERABILITY WATCH

Microsoft Patch Tuesday March 2026

Microsoft's March 2026 Patch Tuesday addressed 77–79 vulnerabilities, including eight critical-severity flaws and two zero-days. A significant focus was placed on Microsoft Office and SQL Server, with Elevation of Privilege (EoP) and Remote Code Execution (RCE) vulnerabilities comprising the majority of the release. Key critical RCEs include CVE-2026-26110 (type confusion) and CVE-2026-26113 (untrusted pointer dereference), both affecting Office and triggerable via the preview pane. Additionally, Microsoft addressed a publicly disclosed SQL Server EoP (CVE-2026-21262) and a .NET Denial of Service zero-day (CVE-2026-26127). Azure administrators should prioritize fixes for ACI Confidential Containers (CVE-2026-23651 and CVE-2026-26124), which addressed critical privilege escalation risks in serverless environments. CISA has added several of these to its KEV catalog, with remediation deadlines established for late March 2026.

Adobe Patches for March 2026

Adobe's March 2026 update addressed 80 vulnerabilities across eight major product lines, a significant increase in volume compared to the previous month. Critical security bulletins were issued for Adobe Commerce (APSB26-05), Illustrator (APSB26-18), and Acrobat/Reader (APSB26-26). The Acrobat and Reader update is of particular concern, addressing critical RCE and EoP flaws that could be exploited through maliciously crafted PDF documents. Other impacted products include Premiere Pro, Experience Manager, Substance 3D Painter, and the DNG SDK. While no active exploitation was reported at the time of release, the prevalence of Illustrator and Acrobat in corporate workflows makes these high-priority targets for initial access via phishing and file-sharing platforms.

Google Chrome Security Updates March 2026

Google released critical security updates on March 12, 2026, to address two high-severity zero-day vulnerabilities (CVE-2026-3909 and CVE-2026-3910) actively exploited in the wild. CVE-2026-3909 (CVSS 8.8) is an out-of-bounds write vulnerability in the Skia 2D graphics library, while CVE-2026-3910 (CVSS 8.8) involves an inappropriate implementation in the V8 JavaScript engine. Both flaws allow remote attackers to execute arbitrary code within the browser sandbox via specially crafted HTML pages. These represent the third and fourth Chrome zero-days discovered in 2026. CISA has mandated a remediation deadline of March 27, 2026, for federal agencies. All users of Chromium-based browsers—including Microsoft Edge, Brave, and Opera—should ensure they have updated to version 146.0.7680.75 or later to mitigate these risks

SECURITY ADVISORIES

Key Recommendations to Protect Your Business

Deploy Phishing-Resistant MFA and Identity Threat Detection (ITDR)

With 82% of intrusions now being malware-free and identity misuse driving the majority of initial access, traditional multi-factor authentication is no longer a sufficient defense against sophisticated adversaries. Organizations should transition to phishing-resistant authentication methods, such as FIDO2-compliant hardware keys, to eliminate the risk of adversary-in-the-middle (AiTM) and session hijacking attacks. Beyond the login phase, implementing Identity Threat Detection and Response (ITDR) is essential to monitor for behavioral anomalies within "valid" sessions. These tools can detect unauthorized session token reuse or sudden administrative privilege escalation in real-time. Integrating ITDR with automated response playbooks allows security teams to instantly terminate suspicious sessions or enforce step-up authentication, directly addressing the threat of rapid lateral movement.

Enhance Forensics Readiness through Centralized Log Orchestration and PII Masking

Given the strict 6-hour reporting window mandated by CERT-In for major cyber incidents, forensics readiness has become a critical operational requirement. Organizations should implement centralized log orchestration that aggregates telemetry from application backends, cloud service providers, and identity platforms into a tamper-proof, immutable repository. To maintain compliance with the DPDP Act while preserving investigative utility, automated PII masking and tokenization should be applied to sensitive data fields at the point of ingestion. This ensures that forensic investigators can reconstruct attack paths and identify root causes without exposing sensitive customer information. Establishing these controls during the "peace-time" phase significantly reduces the Mean Time to Respond (MTTR) and ensures that regulatory disclosures are both timely and accurate.

CYBER QUIZ

FIND ANSWERS IN
THE NEXT EDITION

A CFO receives a high-quality video call from the CEO requesting an urgent, secret bridge loan payment to a new vendor. Despite the CEO's familiar appearance and voice, which of the following is the most effective "proof-of-life" technique to verify the caller's identity?

a) Asking the caller to confirm their employee ID number
b) Requesting the caller to perform an unexpected physical action, such as turning their head sideways or holding up a specific object
c) Checking if the email address in the calendar invite matches the corporate domain
d) Verifying the urgency of the request against the company's quarterly earnings report

Which identity-centric security model is specifically designed to mitigate "breakout time" by ensuring that even a compromised "legitimate" credential has limited access that expires immediately after a task is completed?

a) Static Multi-Factor Authentication (MFA)
b) Role-Based Access Control (RBAC)
c) Just-In-Time (JIT) Privileged Access Management
d) Perimeter-based Firewall Filtering

ANSWERS FOR MARCH CYBER PLUGGED-IN NEWSLETTER QUIZ

Ans: **C** Introduction of vulnerabilities or malware through unverified dependencies.

Ans: **B** Use of polymorphic malware and lateral movement

GET IN TOUCH:

RUSHIK PATEL
Associate Director
Edme Insurance Brokers Limited
Email: rushik.patel@edmeinsurance.com
Phone: +91 9820390280

ROHIT SHARMA
Cyber Practice Leader
Edme Insurance Brokers Limited
Email: rohit.sharma@edmeinsurance.com
Phone: +91 7009612226

edme

Clarity in Complexity

Edme Insurance Brokers Ltd. (formerly known as Aditya Birla Insurance Brokers Ltd.) | Registered Office: 2nd Floor, Privillion, East Wing, Sarkhej - Gandhinagar Highway, Vikram Nagar, Bodakdev, Ahmedabad, Gujarat 380054 | IRDAI License Number: 146 |Composite Broker | License Valid till: 9th April, 2027 | CIN: U99999GJ2001PLC062239 | Corporate Office: 6th floor, VIOS Tower, Off Eastern Freeway, Near Wadala Truck Terminal, Wadala East, Mumbai- 400037 | Toll free no-1800 120 2510 | W: www.edmeinsurance.com | In case of any queries/complaints/grievances, please write to us at care@edmeinsurance.com I ISO 9001 Quality Management Certified by Intertek Certification Ltd. under certificate number 0145476

ankura®

Edme sourced the above content/ information through Ankura Consulting Group, LLC, an independent Global expert services and advisory firm. For more information, please visit: **www.ankura.com** or email **amit.jaju@ankura.com**