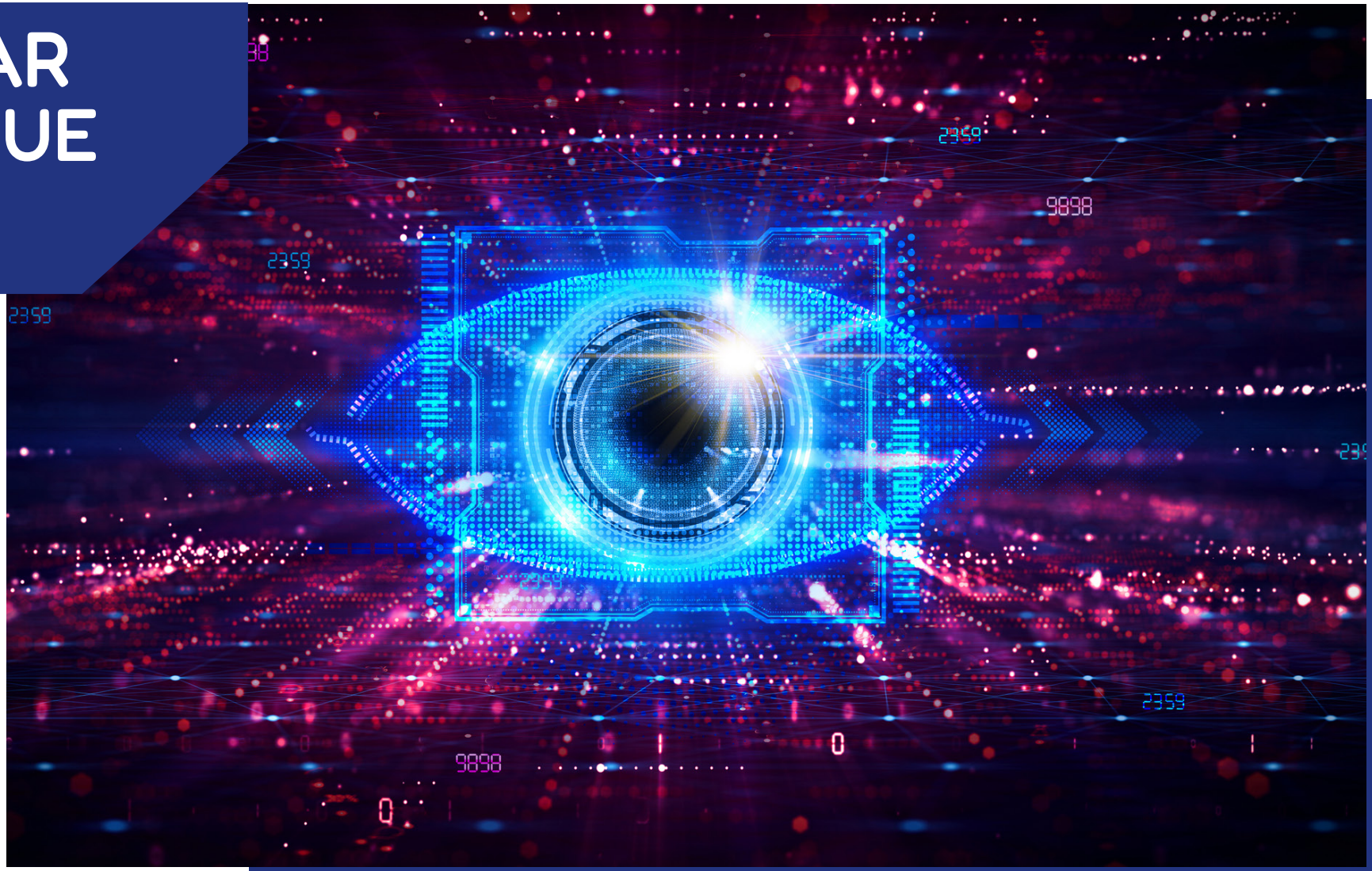
EDME CYBER PLUGG IN
MONTHLY NEWSLETTER
MAR 2026

MAR ISSUE 13



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 "Log-In" Instead of "Break-In" Era:

Initial Access Brokers (IABs) like the threat actor Zestix have industrialized credential theft. In February, major breaches at CarGurus (affecting 12 million users) and Substack were traced back to stolen credentials and API vulnerabilities rather than traditional malware. Attackers are increasingly bypassing the perimeter by using legitimate but compromised access keys.

Identity Fraud & Generative AI Proliferation:

Identity fraud has become a primary financial threat. Fraudsters are now deploying Autonomous AI Fraud Agents that probe defenses and adjust tactics in real-time. In February, research indicated that 1 in 31 GenAI prompts within corporate networks posed a high risk of sensitive data exposure, highlighting the "Shadow AI" risk where employees inadvertently leak proprietary code or PII.

India's New SEBI & CERT-In Mandates:

As of February 2026, SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF) has entered a critical enforcement phase. Regulated entities must now ensure MTTD (Mean Time to Detect) is under 24 hours and critical patches are applied within 14 days. Additionally, CERT-In has reinforced the 6-hour reporting window for all major cybersecurity incidents, placing immense pressure on incident response teams.

Targeted Operational Disruption (Healthcare &

Ransomware groups like Qilin and The Gentlemen have pivoted toward high-pressure targets. In February, the University of Mississippi Medical Center was forced to close clinics and cancel surgeries following a system-wide encryption event. Similarly, Sapienza University of Rome faced days of IT outages, proving that attackers are prioritizing sectors where downtime has the highest human and social cost.

Supply Chain "Cascading" Breaches:

The "Shai-Hulud" NPM malware campaign reached its peak this month, impacting over 800 packages and 700 organizations. By compromising upstream open-source components, attackers inherited "trusted access" to thousands of downstream users, effectively turning a single point of failure into a global systemic risk.

CYBER NEWS

India Faces 3,195 Weekly Cyber Attacks

According to the Check Point 2026 Cyber Security Report, Indian organizations are now facing an average of 3,195 attacks per week, a 2% increase year-over-year. The report highlights that the Education (7,684 attacks) and Business Services (3,747 attacks) sectors are the most frequent targets. Attackers are increasingly using AI-driven automation to scale reconnaissance and execute multi-channel campaigns across email web, and phone.

READ MORE >

Escalation of AI-Driven "Agentic" Phishing

In January, domestic security analysts documented a shift from static phishing to "Agentic AI" campaigns. Unlike traditional scams, these autonomous AI agents can engage in real-time, multi-turn conversations with employees via chat and email, adapting their persuasion tactics based on the victim's responses. This method has proven highly effective at bypassing standard behavioral filters, as the AI mimics internal organizational context and regional language nuances with high precision.

READ MORE >

Shift Toward Edge AI for Enhanced Security Control

A January report highlighted that 91% of cyber detections in India still originate from on-premise environments, pointing to significant risks in legacy infrastructure. The rapid adoption of connected "Smart City" and industrial IoT (Internet of Things) devices has outpaced the implementation of strong authentication and encryption. Experts warn that as these systems become more integrated, the potential for a localized breach to cause large-scale operational disruption across utilities and transportation has reached a critical level.

READ MORE >

Schneider Prototyping Ransomware Attack

The Indian arm of Schneider Prototyping was hit by the Black Shrantac ransomware group. The attackers claimed to have exfiltrated 2TB of sensitive data, including financial records and CXO-level internal communications, highlighting vulnerabilities in India's high-end manufacturing sector.

READ MORE >

Transition to Immutable Data Protection Models

Following a series of targeted attacks in early January, Indian firms are rapidly adopting "Immutable Backups" as a standard defense against modern extortion. Unlike traditional backups, which attackers often seek to encrypt or delete first, immutable storage prevents any modification or deletion of data for a set period. This architectural change ensures that even if administrative credentials are compromised, the organization retains a guaranteed, tamper-proof recovery point.

READ MORE >

CYBER NEWS

Operation Cyber Guardian: The Singapore Telco Siege

The Cyber Security Agency of Singapore (CSA) revealed a massive state-sponsored campaign where the threat group UNC3886 maintained a "silent presence" within major telecommunications providers for nearly a year. Using custom rootkits to bypass traditional perimeter security, the attackers focused on strategic persistence and espionage rather than immediate data theft.

READ MORE >

University of Mississippi Medical Center Shutdown

A severe ransomware attack in mid-February crippled the IT systems and Electronic Health Records (EHR) of the University of Mississippi Medical Center. The incident forced the statewide closure of clinics and the cancellation of multiple surgeries. Operations did not fully recover until early March, highlighting the critical physical stakes of modern healthcare breaches.

READ MORE >

CarGurus Data Breach Impacts 12 Million Users

The online automotive marketplace CarGurus confirmed a major security compromise affecting over 12 million registered users. The breach, first identified by consultant Troy Hunt, exposed a vast amount of Personally Identifiable Information (PII) including names, email addresses, and phone numbers. The incident has already sparked multiple class-action lawsuits.

READ MORE >

INTERPOL Operation Red Card 2.0 Results in 651 Arrests

Concluding on January 30 with results publicized in February, Operation Red Card 2.0 targeted transnational fraud across 16 African countries. The crackdown resulted in 651 arrests and the recovery of $4.3 million. Investigators linked the targeted scam networks to over $45 million in global losses from high-yield investment and mobile money fraud.

READ MORE >

Zero-Day Exploitation of Dell RecoverPoint

A critical zero-day vulnerability (CVE-2026-22769) in Dell RecoverPoint for Virtual Machines was found to be under active exploitation by a suspected China-linked group, UNC6201. The flaw allows for unauthorized root access via hard-coded credentials, enabling the deployment of stealthy backdoors like "BRICKSTORM" within virtualized environments.

READ MORE >

01
CASE STUDY

Brief Summary:

A mid-sized healthcare BPO servicing multiple hospital networks across India and the Middle East was struck by a ransomware attack in early Feb 2026. Attackers gained initial access through a dormant vendor account belonging to a decommissioned medical transcription partner whose VPN credentials had never been revoked. Over 18 days of undetected dwell time, the threat actors exfiltrated 380GB of patient health records, insurance claims data, and billing system exports before deploying encryption payloads that took down the claims processing platform for six business days.

Root Cause Analysis:

Vendor Lifecycle Management:
A decommissioned third-party account remained active for 14 months due to a lack of automated off-boarding processes upon contract termination.

Network Architecture:
A flat internal network with no micro-segmentation allowed the attacker to move laterally from administrative systems into sensitive clinical environments without resistance.

Security Monitoring:
SIEM alert fatigue resulted in 47 anomalous access indicators being deprioritized and ignored over an 18-day dwell period, preventing human intervention.

Loss and Insurance Applicability:

- The six-day claims processing outage triggered contractual penalty clauses with three hospital clients, resulting in direct financial liability.
- The exposure of patient health records (PHI) and insurance data across two jurisdictions created simultaneous regulatory breach notification obligations under India's DPDP Act and UAE healthcare data regulations, requiring engagement of external legal counsel in both countries.
- Insurance Applicability: The claim was partially contested under the 'Third-Party Access Controls' warranty in the cyber policy. The insurer noted that the absence of any quarterly vendor access audit a condition explicitly listed in the policy schedule constituted a material breach of warranty, resulting in a 30% co-insurance penalty on the total claim payout.

Recommended Post-Incident Measures:

Automated Vendor Off-boarding: Implement an identity governance platform that automatically triggers credential revocation and VPN access termination upon contract expiry or vendor relationship closure, with a maximum 24-hour grace period for documented exceptions.

Network Micro-segmentation: Isolate clinical data environments from administrative and billing systems using zero-trust network access principles, ensuring that any single compromised account cannot reach both PHI and financial systems simultaneously.

SIEM Tuning & Tiered Alert Escalation: Establish mandatory escalation SLAs for alerts involving privileged or third-party accounts—any anomalous access event from an external entity must trigger a Tier-2 analyst review within 4 hours regardless of severity classification.

02
CASE STUDY

Brief Summary

A regional non-banking financial company (NBFC) operating across western India suffered a Business Email Compromise (BEC) attack that resulted in an unauthorised wire transfer of ₹2.3 crore to an overseas account. Attackers used an AI-generated voice clone of the CEO created from publicly available earnings call recordings to instruct the CFO over a WhatsApp voice note to urgently approve an 'undisclosed acquisition payment.' The voice note was accompanied by a spoofed email thread that appeared to originate from a legitimate external legal counsel domain.

Root Cause Analysis:

Deepfake Voice Cloning:
Threat actors utilized AI voice synthesis to replicate the CEO's accent and style from public media, successfully bypassing cognitive filters during the impersonation.

Verification Gaps:
The organization lacked a mandatory out-of-band call-back protocol, allowing high-value financial transfers to proceed without independent verification via a second communication channel.

Email Security Failures:
A lack of DMARC 'reject' enforcement and gaps in the email gateway allowed a newly registered spoofed domain to pass security checks and reach the CFO.

Loss and Insurance Applicability:

- ₹2.3 crore was transferred to a layered overseas account structure. Of this, ₹1.1 crore was recovered through a rapid banking freeze request coordinated with the RBI Ombudsman within 6 hours of discovery.
- The residual ₹1.2 crore loss, along with forensic investigation and legal costs, was submitted under the 'Social Engineering Fraud' coverage in the firm's cyber insurance policy.
- Insurance Applicability: The claim was accepted in full. The policy's social engineering fraud sublimit covered up to ₹2 crore. The insurer noted, however, that the absence of a documented dual-authorisation protocol for wire transfers above ₹50 lakh would be a mandatory security control requirement at renewal, with non-compliance triggering a 25% premium surcharge.

Recommended Post-Incident Measures:

Out-of-Band Verification: Implement a mandatory policy requiring direct phone confirmation for all financial instructions exceeding ₹25 lakh. Verification must use pre-registered corporate directory numbers rather than contact details provided within the request.

DMARC Enforcement: Upgrade domain security policies from monitoring to 'p=reject' across all corporate domains. This should include the defensive registration of typosquatted domain variants to prevent spoofing and impersonation.

Deepfake Awareness Training: Establish quarterly tabletop exercises for finance, legal, and C-suite teams focusing on AI voice and video impersonation. Staff should be trained to treat high-urgency, high-value requests outside standard channels as immediate red flags.

DATA SPOTLIGHT

The Convergence of AI Offence, Credential Markets & Third-Party Exposure

Supporting Statistics:

- The 29-Minute Breakout Benchmark: The average "breakout time"—the gap between an attacker's initial entry and their first lateral move—has plummeted to just 29 minutes. This represents a 65% increase in speed over 2024, with the fastest recorded breakout in February occurring in a staggering 27 seconds.
- Identity as the Primary Vector: Identity weaknesses played a material role in 89% of all incident investigations this month. Instead of technical exploits, 65% of initial access is now driven by "legitimate" credential misuse, session token theft, or sophisticated social engineering.
- The Browser as the New Battlefield: Approximately 48% of all attacks in February involved the browser. Routine web sessions are being weaponized to harvest credentials and bypass local security controls, making the browser the single most targeted enterprise application.
- SaaS Supply Chain Surge: Attacks involving third-party SaaS integrations have grown 3.8x since 2022. Attackers are increasingly abusing OAuth tokens and API keys to move laterally from trusted vendors directly into primary enterprise environments.
- GenAI Data Leaks: During February, 1 in every 31 GenAI prompts submitted from corporate networks posed a "high risk" of sensitive data exposure. This impacted 88% of organizations that regularly use AI tools, with prompts often containing internal code, credentials, or PII.
- India's Target Density: India recorded the highest average attack volume in the APAC region, with organizations facing 3,195 weekly attacks (+2% YoY). The Education sector remains the prime target, averaging 7,684 attacks per week, followed closely by Government and Business Services.

Implications and Tactical Risks:

- The "Malware-Free" Blind Spot: With 82% of detections now being malware-free, traditional antivirus and EDR tools are increasingly ineffective. Security teams must transition to Identity Threat Detection and Response (ITDR) to monitor for anomalous behavior within "valid" user sessions.
- Vulnerability-to-Exploit Compression: Attackers are now using AI to automate the "monitor-diff -test-weaponize" loop for new CVEs. Scanning for newly announced vulnerabilities often begins within 15 minutes of a public disclosure, often before security teams have finished reading the advisory.
- Agentic Identity Management: As companies deploy autonomous AI agents to handle workflows, these agents are becoming distinct digital actors. The risk of "privilege creep" in AI service accounts necessitates a move toward dynamic, task-specific, and just-in-time (JIT) access for non-human identities.

VULNERABILITY WATCH

Microsoft Patch Tuesday February 2026

Microsoft's February 2026 Patch Tuesday addressed 58–61 vulnerabilities, including five Critical-severity flaws and six actively exploited zero-days (three publicly disclosed prior to patching). Elevation of Privilege dominated at 42% of all CVEs. Key zero-days include a Windows Shell SmartScreen bypass (CVE-2026-21510), an MSHTML security feature bypass (CVE-2026-21513), a DWM EoP via type confusion (CVE-2026-21519), and an RDS EoP (CVE-2026-21533) tied by CrowdStrike to threat actors targeting U.S. and Canadian entities since late December 2025. CISA added four of the six to its KEV catalog with a March 3, 2026 remediation deadline. Microsoft also patched three GitHub Copilot prompt/command injection flaws and began rolling out updated Secure Boot certificates ahead of the June 2026 expiry of the original 2011 certificates.

Adobe Patches for February 2026

Adobe's February 2026 Patch Tuesday addressed 44 vulnerabilities across nine products. Audition, After Effects, InDesign Desktop, Bridge, Lightroom Classic, the DNG SDK, and the three Substance 3D applications with no active exploitation reported at the time of release. Over two dozen CVEs carry Critical ratings, the majority being arbitrary code execution flaws triggered by opening maliciously crafted files. Highest-risk products are After Effects, InDesign, and Bridge, each patched for Critical ACE vulnerabilities. Substance 3D products additionally received fixes for memory exposure and DoS issues. InDesign and After Effects should be prioritised given their prevalence in creative environments where external document-sharing makes malicious file delivery a realistic attack vector.

Google Chrome Security Updates February 2026

Google issued an emergency out-of-band Chrome update on February 13, 2026 to patch CVE-2026-2441 (CVSS 8.8), the first actively exploited Chrome zero-day of 2026. The flaw is a use-after-free vulnerability in the CSSFontFeatureValuesMap component, triggerable by simply visiting a malicious webpage — no further interaction required. Exploitation was confirmed in the wild prior to patching. While Chrome's sandbox limits immediate impact, researchers note UAF flaws are routinely chained with sandbox escapes for full system compromise. All Chromium-based browser users (Edge, Brave, Opera, Vivaldi) should update immediately — Chrome 145.0.7632.75/76 for Windows/macOS, 144.0.7559.75 for Linux — via Chrome Menu > Help > About Google Chrome.

SECURITY ADVISORIES

Key Recommendations to Protect Your Business

Implement Runtime Security Controls for Containerized and Serverless Environments

As organizations adopt microservices, containers, and serverless functions to accelerate digital transformation, traditional security tools often lack the context and visibility needed to protect these dynamic workloads. Implementing runtime security controls is essential to detect and mitigate threats that bypass static scanning. Use behavior-based monitoring to identify anomalies such as unauthorized system calls, code injection attempts, or lateral movement within container clusters. Integrate host-based intrusion detection systems (HIDS), eBPF-based monitoring, and workload protection platforms with orchestration layers like Kubernetes or OpenShift. These controls should enforce automated responses — such as isolating containers, terminating suspicious processes, or alerting SOC teams — to prevent attacks from propagating in production environments.

Apply Granular Data Classification and Tokenization Across Data Flows

Securing sensitive data requires more than encryption at rest and in transit. Organizations should deploy advanced data classification technologies that automatically discover, tag, and categorize data based on business sensitivity, regulatory exposure, and contextual usage. This classification should drive downstream protection mechanisms, including dynamic tokenization, format-preserving encryption (FPE), and fine-grained access controls. Apply these protections throughout the data lifecycle — from ingestion through processing and storage — especially across APIs and third-party integrations. Integrating tokenization at the application layer helps reduce compliance scope (e.g., PCI DSS) while preserving data utility for analytics and operational use.

CYBER QUIZ

FIND ANSWERS IN
THE NEXT EDITION

In a containerized environment, which security risk is most associated with using publicly available container images without proper validation?

a) Data exfiltration through encrypted channels
b) Unauthorized access via misconfigured firewall rules
c) Introduction of vulnerabilities or malware through unverified dependencies
d) Excessive identity federation across cloud platforms

Which of the following techniques is commonly used in advanced persistent threats (APTs) to maintain long-term access within a targeted network without detection?

a) Brute-force password attacks
b) Use of polymorphic malware and lateral movement
c) Simple phishing emails with public links
d) Exploiting outdated web browser plugins.

ANSWERS FOR February CYBER PLUGGED-IN NEWSLETTER QUIZ

Ans: **C** Decline the request, hang up, and call the provider's official support number to verify the claim.

Ans: **B** Symmetric encryption uses one private key for both locking and unlocking; Asymmetric uses a public/private key pair.

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**