

**JULY
ISSUE
17**



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

Third-Party SaaS Platforms Become the Preferred Ransomware Entry Point

In June 2026, extortion groups increasingly bypassed hardened perimeters by targeting SaaS vendors. ShadowByt3\$ breached Nintendo through TinyPulse, a third-party employee-engagement platform, exfiltrating ~859 MB of HR data and demanding USD 2 million; when refused, it redirected the demand to the vendor itself. Vendor-side SaaS integrations, not the primary target's network, are now a leading initial-access route.

Healthcare and Data-Extortion Campaigns Accelerate Under ShinyHunters

ShinyHunters continued its pay-or-leak campaign, claiming theft of 8.8 TB from Amazon-owned One Medical Seniors and listing Kodak and Madison Square Garden Entertainment on its leak site. None of the claims are independently verified, but its focus on big-game healthcare and consumer targets, short deadlines, and reputational pressure over encryption shows extortion-only tactics displacing traditional ransomware.

Credential Reuse Eclipses Zero-Days as the Top Perimeter Risk

The FortiBleed campaign harvested valid administrator and VPN credentials for ~86,644 internet-facing Fortinet devices across 194 countries, roughly half the fleet, without exploiting any new vulnerability, combining credential reuse with industrialised brute-force. CISA and the UK NCSC issued advisories on 18 June 2026, reinforcing that identity hygiene, not patch velocity alone, increasingly decides whether perimeter devices hold.

AI Browsing Agents Emerge as a Novel Remote-Code-Execution Vector

Microsoft disclosed AutoJack, an exploit chain showing how a single malicious webpage rendered by an AI browsing agent can reach a privileged local service and run arbitrary code with no credentials and no user interaction. Found in a pre-release AutoGen Studio branch and fixed before release, it signals a structural lesson: once an agent browses the open web and talks to privileged local services, localhost stops being a trust boundary.

Public-Safety and Critical Communication Systems Draw Pure-Disruption Attacks

Brazil's national Civil Defence alert platform was hijacked on 19-20 June 2026, with attackers triggering ten unauthorised "Extreme Alert" messages that bypassed silent mode on millions of phones before the system was taken offline. With no ransom or data theft reported, the attack appears aimed purely at disruption, a reminder that critical communication and public-warning systems are increasingly viable targets.

CYBER NEWS



Nintendo Breach Exposes Risk of Third-Party HR Platforms

The extortion group ShadowByt3\$ claimed a breach of Nintendo via TinyPulse, a third-party employee-engagement platform, in mid-June 2026, alleging theft of approximately 859 MB of HR data including employee names, survey responses, and financial records dating back to 2016. Nintendo confirmed an incident but said it was limited to a small subset of historical internal survey content and that its own systems, along with customer and financial data, were unaffected. After Nintendo declined a USD 2 million ransom, the group redirected its extortion demand to TinyPulse itself, illustrating the growing practice of pressuring downstream SaaS vendors when the primary target will not pay.

[READ MORE >](#)

ShinyHunters Claims 8.8 TB Theft From Amazon's One Medical

Amazon-owned One Medical disclosed that an unauthorised party accessed a third-party file-storage system holding archived records of One Medical Seniors (formerly Iora Health) patients between 8 and 11 June 2026. The extortion group ShinyHunters subsequently claimed responsibility and threatened to publish 8.8 TB of allegedly stolen data, giving the company until 22 June 2026 to begin negotiations. One Medical said the exposure was limited to legacy Iora Health patient files across nine clinic markets and that its core electronic medical record system was unaffected; it has revoked access and rotated credentials across the affected platform.

[READ MORE >](#)

FortiBleed Exposes Credentials for 86,644 Fortinet Devices Worldwide

Security researchers uncovered an exposed threat-actor server hosting a continually updated database of verified FortiGate administrator and VPN credentials, harvested through a combination of credential reuse, brute-force attacks, and offline hash-cracking against an estimated 86,644 devices in 194 countries. CISA and the UK National Cyber Security Centre issued joint advisories on 18 June 2026 urging organisations to terminate active sessions, reset all administrative and VPN credentials, enforce MFA, and migrate to PBKDF2-based password hashing. Fortinet clarified that the campaign does not stem from a new software vulnerability, meaning there is no single patch that closes it.

[READ MORE >](#)

International Operation Endgame Dismantles SocGhosh Malware Network

Law enforcement agencies from the Netherlands, Canada, the United States, and Germany, supported by Europol, announced on 18 June 2026 the disruption of TA569, the threat actor behind the SocGhosh ("FakeUpdates") malware framework. The action seized more than 100 servers and domains and remediated nearly 15,000 compromised WordPress websites used to serve fake browser-update lures. SocGhosh has functioned as a leading initial-access broker for ransomware operators, including Evil Corp, for almost a decade, and investigators recovered 1.4 million leaked website credentials during the operation.

[READ MORE >](#)

Brazil Suspends National Emergency Alert System After Suspected Cyberattack

Brazil's Civil Defence alert platform was compromised overnight on 19-20 June 2026, with attackers issuing ten unauthorised "Extreme Alert" notifications to phones across several states, overriding silent-mode settings with no genuine disaster underway. The federal government suspended the platform and is investigating with federal police; officials said the alert-composition interface, not the underlying broadcast standard, had been breached by someone outside the national civil defence network. The incident underscores the disruption risk to public-warning systems that are deliberately designed to override user controls during emergencies.

[READ MORE >](#)

CYBER NEWS



RBI Releases Draft Guidance on Model Risk Management, Including AI/ML Kill Switches

On 24 June 2026, the RBI published a draft "Guidance on Regulatory Principles for Model Risk Management, 2026," extending governance requirements beyond credit models to all models, including AI and machine learning systems, used by eleven categories of regulated entities. The draft requires a board-approved Model Risk Management Framework, validation of high-risk models by the Risk Management Committee of the Board before deployment, continuous monitoring of third-party and AI-based models, and the ability to restrict or disable models that pose unacceptable risk. Public comments are invited until 24 July 2026.

[READ MORE >](#)

MHA's I4C Warns of 'Boss Scam' CEO-Impersonation Fraud Targeting Corporates

The Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs, issued an advisory on 22 June 2026 describing a fraud pattern dubbed the "Boss Scam," in which attackers impersonate regulators such as the RBI to trick senior executives into opening a malicious archive over email or WhatsApp. The resulting malware hijacks the executive's active WhatsApp Web session, which attackers then use to instruct finance teams to authorise fraudulent transfers, in some cases altering saved contact names to reinforce the impersonation. I4C has urged organisations to mandate out-of-band voice or in-person verification for any payment instruction received over messaging platforms and to restrict execution of unknown files from user-profile directories.

[READ MORE >](#)

CERT-In Flags Large-Scale Malware Campaign Targeting WhatsApp Web and Desktop Users

In an advisory dated 25 June 2026, CERT-In warned of a large-scale campaign spreading malicious VBScript files via direct messages from compromised WhatsApp accounts, affecting both Web and desktop clients. Infection can give attackers remote device access, harvest credentials, deploy further malware, and spread to contacts. Echoing I4C's Boss Scam warning, CERT-In urges users not to open unexpected attachments, even from trusted contacts.

[READ MORE >](#)

RBI Sets 30 June Deadline for Board-Approved AI Cybersecurity Gap Assessments

The Reserve Bank of India has directed banks and other regulated entities to complete a board-approved gap assessment of risks posed by frontier AI models and submit a time-bound corrective action plan by 30 June 2026. The mandate requires regulated entities to establish a structured cybersecurity framework, conduct AI-led adversarial testing of internet-facing infrastructure, and identify vulnerabilities such models could exploit, with sign-off required at board level. The directive follows earlier RBI advisories on frontier AI risk and reflects growing regulatory concern that AI-assisted vulnerability discovery is compressing the time between exposure and exploitation in the financial sector.

[READ MORE >](#)

Tata Electronics Confirms Cyberattack After Apple, Tesla Documents Surface Online

Tata Electronics, a key Apple iPhone assembly partner and supplier to Tesla, confirmed a cybersecurity incident after the extortion group World Leaks published material on the dark web that researchers say includes documents bearing Apple's and Tesla's proprietary markings, including quality-inspection standards and component drawings. The data had reportedly been accessible on the dark web since at least 10 June 2026. Tata Electronics said its response protocols were activated immediately and that the incident has not affected operations across its businesses; the episode highlights the concentrated supply-chain exposure created when a small number of Indian contract manufacturers hold sensitive design data for multiple global technology and automotive clients.

[READ MORE >](#)

01 CASE STUDY

Brief Summary:

A mid-sized Non-Banking Financial Company (NBFC) operating consumer lending and payroll-linked loan products across western India experienced a targeted fraud incident that originated not in its own network, but in a third-party HR analytics platform used to administer employee engagement surveys. Attackers compromised the vendor's cloud environment and exfiltrated a dataset containing the NBFC's employee names, designations, official email addresses, and partial salary-band information. Roughly three weeks later, the company's Chief Financial Officer received a WhatsApp message, apparently from the Managing Director, referencing an urgent RBI compliance deadline and containing a compressed attachment. Opening the file on a Windows laptop installed a trojan dropper that hijacked the CFO's active WhatsApp Web session. Messages sent from the CFO's genuine account then instructed two members of the finance team to process an urgent vendor payment of Rs 2.3 crore to an account later traced to a money-mule network.



Root Cause Analysis:

Third-Party Vendor Without Security Due Diligence:

The HR analytics platform had been onboarded without a documented vendor risk assessment or contractual security requirements, despite holding identifiable employee data for the entire organisation.

No Out-of-Band Verification for Payment

Instructions: The finance team's standard operating procedure permitted payment authorisation based on a WhatsApp message from a recognised contact, without a parallel voice or in-person confirmation step.

Absence of Endpoint Detection on Executive Devices:

The CFO's laptop ran signature-based antivirus only; the trojan dropper's behaviour, hijacking an active messaging session rather than exfiltrating files directly, did not trigger any alert.

Loss and Insurance Applicability:

- Direct loss from the fraudulent transfer totalled Rs 2.3 crore, of which approximately Rs 40 lakh was recovered through a freeze order obtained via the National Cybercrime Reporting Portal before the remaining funds were dispersed across multiple accounts. The NBFC's cyber insurance policy responded under Social Engineering Fraud and Computer Crime coverage, though the insurer applied a sub-limit specific to fund-transfer fraud that capped recovery at 50% of the insured loss, as the policy's underlying control requirements specified callback verification for any transfer above Rs 25 lakh, a control that had not been consistently enforced.

Recommended Post-Incident Measures:



Vendor Risk Assessment for All Third-Party SaaS Platforms: Extend the existing vendor risk management programme to HR, payroll, and engagement-survey platforms, requiring evidence of access controls and breach-notification commitments before onboarding.



Out-of-Band Verification for High-Value Payment
Instructions: Mandate independent voice or in-person confirmation, using contact details verified outside the originating channel, for any payment instruction received over WhatsApp, SMS, or email above a defined threshold.



Behavioural Endpoint Detection on Privileged and Executive Devices: Deploy EDR with behavioural detection capable of flagging session-hijacking and unauthorised process injection on devices used by finance and executive staff.

02 CASE STUDY

Brief Summary

A mid-sized private sector bank's regional data centre suffered a ransomware incident that traced back to a FortiGate SSL VPN appliance whose administrator credentials had never been rotated since deployment four years earlier. Unknown to the bank's security team, those credentials had been harvested during an earlier, unrelated breach of a partner organisation and had been circulating in criminal credential marketplaces for several months. Attackers logged into the VPN appliance directly, using valid credentials and no exploit, then used the foothold to move laterally into the bank's regional reporting and reconciliation servers over a 36-hour window before deploying ransomware that encrypted those systems at two regional offices. Customer-facing core banking and payment switch infrastructure, which sat on a segmented network, was not affected.



Root Cause Analysis:

Stale, Never-Rotated Perimeter Credentials:

VPN administrator credentials had remained unchanged since initial deployment, with no periodic rotation policy in place for network appliance accounts.

No Multi-Factor Authentication on the VPN Administrative Interface:

The appliance's administrative and SSL VPN logins relied on password authentication alone, allowing the attacker to authenticate successfully with no further challenge.

Insufficient Network Segmentation Between Regional Offices: While core banking systems were isolated, regional reporting and reconciliation servers shared a flat network with the compromised VPN appliance, allowing lateral movement without further exploitation.

Loss and Insurance Applicability:

- The incident resulted in an estimated loss of Rs 6.1 crore, comprising forensic investigation, system rebuild, regulatory notification to the RBI and CERT-In, customer communication, and four days of reduced reconciliation capacity at the affected offices. The bank's cyber insurance policy responded under Network Security Liability and Business Interruption, with the insurer funding incident response and legal costs in full; however, a co-insurance clause tied to the policy's MFA warranty reduced the business interruption payout by 20%, since the warranty had specified MFA on all internet-facing administrative interfaces.

Recommended Post-Incident Measures:



Mandatory MFA on All Perimeter and Administrative Interfaces: Enforce phishing-resistant multi-factor authentication on every internet-facing VPN, firewall, and administrative login, with no exceptions for legacy appliances.



Scheduled Credential Rotation for Network Appliances: Implement a fixed rotation cycle for all firewall, VPN, and network-device administrative credentials, independent of staff turnover triggers alone.



Network Segmentation Aligned to Data Sensitivity, Not Just System Criticality: Extend segmentation controls to regional reporting and reconciliation systems, which, while not customer-facing, can still serve as a lateral-movement path into sensitive environments.

DATA SPOTLIGHT

The Exposure Gap — Why Patching Speed and Vendor Identity Now Decide Breach Outcomes

Supporting Statistics:

- **Vulnerability Exploitation Overtakes Credential Abuse (Verizon 2026 DBIR):**
Exploitation of vulnerabilities hit 31% of initial access (up from 20%, +55% YoY), overtaking credential abuse, which fell to 13%.
- **Credentials Still Dominate the Full Attack Chain (Verizon 2026 DBIR):**
Credential abuse appears in 39% of breaches end-to-end — initial access and lateral movement remain distinct problems.
- **Malware Is Optional Now (CrowdStrike 2026 Global Threat Report):**
82% of 2025 detections were malware-free, driven by valid credentials, trusted identity flows, and SaaS abuse. Cloud-conscious intrusions rose 37% (266% among state-nexus actors).
- **Patch Backlogs Are Widening (Verizon 2026 DBIR):**
Only 26% of CISA KEV vulnerabilities were fully remediated in 2025 (down from 38%); median resolution time rose to 43 days from 32.
- **Third-Party Compromise Is a Top-Tier Vector (Mandiant M-Trends 2026):**
17% of cloud IR cases 2nd most common, behind voice phishing (23%) — visible this month in the Nintendo/TinyPulse and Tata Electronics incidents.
- **Dwell Time Rose (Mandiant M-Trends 2026):**
Global median dwell time climbed to 14 days from 11, as espionage actors get stealthier post-access.

Implications and Tactical Risks:

- **Vendor Risk Is First-Party Risk:**
Third-party compromise now ranks top-three across both Mandiant and Verizon data SaaS integrations need internal-grade monitoring.
- **Credential Hygiene Rivals Patch Velocity:** FortiBleed proved patched fleets still fall to reused credentials; CrowdStrike's 82% figure confirms this is the norm, not the exception.
- **The Patch Gap Is Structural:**
With most KEVs still open a week post-detection, exposure prioritization not faster patching alone is the fix.
- **Rising Dwell Time Is the Quiet Counter-Trend:** Detection tuned only for fast breakout may miss slower, persistence-focused intrusions.

VULNERABILITY WATCH



Microsoft Patch Tuesday June 2026

Microsoft's June 2026 Patch Tuesday addressed 206 vulnerabilities by Microsoft's own count, the largest single monthly release since the program began in 2003, with third-party trackers citing figures between 198 and 208 depending on counting methodology. The release included 33 critical vulnerabilities and three zero-day flaws that were publicly disclosed or known to attackers ahead of patch availability, including a Windows CTFMON elevation-of-privilege bug and an HTTP.sys denial-of-service flaw dubbed "HTTP/2 Bomb." Elevation-of-privilege vulnerabilities again dominated the release at 63 CVEs, while Remote Desktop Client and Windows Hyper-V each received clusters of critical remote-code-execution fixes, the latter capable of enabling VM guest escape. Security teams should prioritise BitLocker, HTTP.sys, Remote Desktop, and Hyper-V hosts given the volume of critical and actively-targeted components in this release.



Adobe Security Updates June 2026

Adobe's June 2026 updates, released alongside Microsoft's Patch Tuesday on 9-10 June, addressed 123 vulnerabilities across eleven product lines, including Experience Manager, Experience Manager Forms, InDesign, InCopy, Substance 3D Sampler, Content Credentials SDK, Dreamweaver, Acrobat Reader, ColdFusion, Format Plugins, and Campaign Classic. Forty-seven of these vulnerabilities were rated critical, with the potential for arbitrary code execution if exploited. Adobe ColdFusion 2025 and 2023 also received a parallel security update the same day, addressing flaws tied to arbitrary code execution, arbitrary file write, and security feature bypass, alongside an upgrade of the underlying Tomcat engine. Adobe reported no evidence of in-the-wild exploitation for any of the June vulnerabilities, though enterprises running ColdFusion or Experience Manager in production should prioritise patching given the critical-severity concentration.



Google Chrome Security Updates June 2026

Google issued two notable Chrome security releases in June 2026. Mid-month, Chrome 149 was updated to fix 74 vulnerabilities, including CVE-2026-11645, a high-severity V8 engine flaw under active exploitation in the wild and subsequently added to CISA's Known Exploited Vulnerabilities catalogue with a remediation deadline of 23 June. A second update on 23-24 June (Chrome 149.0.7827.196/197) addressed a further 18 vulnerabilities, including four rated critical: two WebGL use-after-free flaws (CVE-2026-13028, CVSS 9.6, and CVE-2026-13032) capable of sandbox escape via a crafted webpage, an out-of-bounds read in Blink's InterestGroups component, and a use-after-free in the Autofill subsystem. No active exploitation has been confirmed for the later batch, but the concentration of use-after-free flaws across WebGL, Autofill, and DevTools again underscores why Chromium-based browsers, including Edge, Brave, and Opera, remain a high-frequency patching priority.

SECURITY ADVISORIES

Key Recommendations to Protect Your Business

Treat Third-Party SaaS and Vendor Integrations as a First-Class Attack Surface

June 2026's parade of vendor-side incidents, the Nintendo/TinyPulse breach, Tata Electronics' supply-chain exposure, and the Verizon DBIR's finding that 48% of breaches now involve a third party, make clear that an organisation's security perimeter no longer ends at its own infrastructure. The foundational requirement is a current inventory of every SaaS platform, vendor integration, and managed service connection that touches employee or customer data, paired with a documented vendor risk assessment before onboarding and at defined renewal intervals.

Once visibility is established, organisations should require evidence of access controls, encryption, and breach-notification commitments from vendors handling identifiable employee or customer data, with HR, payroll, and engagement platforms held to the same standard as customer-facing systems. Where a vendor breach does occur, incident response plans should explicitly address downstream fraud risk, particularly social-engineering attempts that weaponise exfiltrated employee data, rather than treating the vendor incident as someone else's problem. Board-level reporting on third-party risk exposure should become a standing item, not a response to a specific incident.

Align Perimeter Credential Hygiene with CERT-In and RBI's AI-Era Expectations

FortiBleed's compromise of roughly half the internet-facing Fortinet fleet without a new vulnerability, combined with RBI's 30 June deadline for board-approved AI cybersecurity gap assessments, points to the same underlying expectation: organisations, particularly in India's financial sector, can no longer treat perimeter device credentials as a set-and-forget control. Every internet-facing firewall, VPN gateway, and administrative interface should be inventoried, with MFA enforced on all of them and a fixed rotation cycle applied to administrative credentials independent of staff turnover. For RBI- and SEBI-regulated entities, the gap assessment now underway should explicitly test whether AI-assisted credential-cracking and brute-force techniques, of the kind used in FortiBleed, could succeed against the organisation's own perimeter estate, and document remediation timelines consistent with CERT-In's tiered, 12-hour-to-5-day containment expectations for known exploited vulnerabilities. Where legacy appliances cannot support modern authentication, temporary compensating controls, network segmentation, IP allow-listing, or enhanced session monitoring, should be documented and time-bound pending replacement.



CYBER QUIZ

FIND ANSWERS IN
THE NEXT EDITION

A mid-sized organisation outsources its employee engagement and survey programme to a third-party SaaS platform that holds employee names, email addresses, and partial financial details for payroll verification. The vendor is later compromised, and the organisation's employee data is exfiltrated, though the organisation's own network is never touched. Three weeks later, an executive receives a WhatsApp message, apparently from a colleague, referencing the breach and requesting an urgent file review. Which combination of controls would have most reduced the organisation's overall exposure to this scenario?

- A. Relying on the vendor's own security certification as sufficient assurance, with no independent review.
- B. Conducting a documented vendor risk assessment before onboarding any platform that holds employee data, contractually requiring breach notification within a defined window, and training staff to treat any unsolicited file-review request referencing a known incident as a potential social-engineering attempt requiring out-of-band verification.
- C. Terminating the vendor relationship immediately after the breach, with no further action.
- D. Restricting the survey platform's use to non-management staff only.

An organisation discovers that its internet-facing FortiGate VPN appliance has valid, working administrator credentials that were never rotated since deployment, and that those credentials appear in a leaked threat-actor database, despite the appliance running fully patched firmware with no known unpatched CVE. Which response addresses the actual root cause of this exposure?

- A. Wait for Fortinet to release a patch, since no vulnerability has been confirmed.
- B. Immediately reset all administrative and VPN credentials, enforce phishing-resistant MFA on the administrative interface, migrate to modern password hashing where supported, and establish a fixed credential rotation cycle for all network appliances going forward.
- C. Increase the firewall's logging verbosity and continue monitoring without changing any credentials.
- D. Restrict the VPN to a single named administrator account to reduce the number of credentials in scope.

ANSWERS FOR JUNE CYBER PLUGGED-IN NEWSLETTER QUIZ

Ans: **B** Pinning all dependency versions in the SBOM, enforcing cryptographic hash verification of packages at install time, and running runtime behavioral monitoring for unexpected outbound network calls from the scanner process.

Ans: **B** Create a pre-authorized emergency change process specifically for CISA/CERT-In KEVs, using automated isolation or WAF-based virtual patching as the immediate 12-hour response, with full patch deployment following the tiered CERT-In schedule under an expedited 4-hour CAB track.



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

GET IN
TOUCH:



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 | ISO 9001 Quality Management Certified by Intertek Certification Ltd. under certificate number 0145476

Edme Insurance Brokers Limited (EIBL) is sharing this advisory/guide to provide general information/awareness for its users, and it should not be construed as technical or professional advice of any manner. The information and descriptions contained herein are not intended to be complete descriptions of all terms as required under the Insurance Policy document to claim for damages/losses. Processing of claim settlement is always subject to applicable terms and conditions of your Insurance Policy and at the discretion of your Insurer on acceptance of such claim. In no event EIBL or its employees shall be responsible or liable for use of such information. You are requested to use your own independent sources diligently.

The trademarks, logos, and brand names of the third parties are used for identification purposes only and in no manner it should be construed or comprehended for any type of endorsement or affiliation or tie-ups for any commercial purpose/use or otherwise.



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