CYBER INSIGHTS DIGEST

OCTOBER EDITION

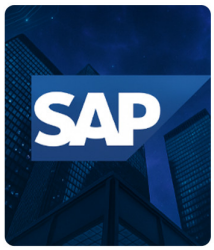
NEWS BYTES - DOMESTIC

CBI Raids 89 Locations in Nationwide Crackdown on Digital-Arrest Scams



Central Bureau of Investigation searched 89 locations across 20 states and arrested three individuals in three digital-arrest cases involving alleged losses of ₹42.36 crore. The operation focused on tracing mule accounts, financial beneficiaries and the wider networks used to receive, layer and disperse fraud proceeds.

CERT-In Issues High-Severity Advisory for SAP Products



The advisory identified vulnerabilities across multiple enterprise products that could enable unauthorized access, arbitrary-code execution, sensitive-data exposure and denial-of-service attacks. Organizations using affected SAP systems were urged to review the risks and implement the appropriate security updates.

CERT-In Flags Actively Exploited Microsoft Vulnerabilities



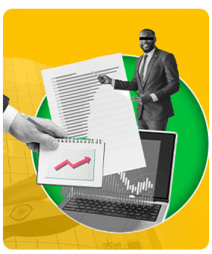
The high-severity advisory warned of vulnerabilities enabling privilege escalation, remote-code execution, information disclosure and system compromise. With certain flaws reportedly exploited in the wild, CERT-In advised users and administrators to apply the relevant security patches immediately.

Government Highlights IMEI Tampering as a Threat to Digital Sovereignty



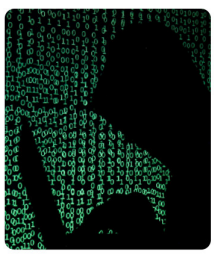
The factsheet highlighted how altered device identities can undermine telecom security, law-enforcement traceability and consumer protection. It also emphasised the shared responsibility of manufacturers, importers, sellers and users in maintaining the integrity of India's mobile-device ecosystem.

SEBI Proposes Extending MII Cybersecurity Frameworks to Subsidiaries



The consultation proposes applying information-technology and cybersecurity requirements governing market infrastructure institutions to their subsidiaries. The proposal aims to address interconnected operational risks and establish more consistent cyber-resilience standards across the securities-market ecosystem.

India Emerges as Asia-Pacific's Most Targeted Country for Ransomware



Research identified 24 publicly claimed Indian victims during August, placing India seventh globally amid record ransomware disclosures. India's sizeable manufacturing and IT-services sectors remain particularly exposed to operational disruption, sensitive-data theft and extortion pressure.

CYBER INSIGHTS DIGEST

OCTOBER EDITION

NEWS BYTES - INTERNATIONAL

European Union Opens €96 Million Cybersecurity Funding Call



The funding call supports AI-powered cybersecurity tools, SME resilience, coordinated preparedness testing and regional undersea-cable security hubs. The initiative is designed to strengthen European cyber capabilities across public bodies, critical sectors and organisations covered by NIS 2.

Google, Anthropic and OpenAI Introduce New Cybersecurity AI Models and Access Programmes



The advisory identified vulnerabilities across multiple enterprise products that could enable unauthorized access, arbitrary-code execution, sensitive-data exposure and denial-of-service attacks. Organizations using affected SAP systems were urged to review the risks and implement the appropriate security updates.

US Agencies Warn of Industrial-Scale AI Model Distillation Campaigns



The joint advisory warned that China-based AI companies were systematically extracting capabilities from US frontier models through large-scale distillation activity. CISA, the NSA and the FBI recommended stronger API monitoring, identity controls, rate limiting and detection of proxy-based evasion.

Cybersecurity Companies Island and Cyera Secure $400 Million Each



The article reported separate $400 million funding rounds for enterprise-browser provider Island and data-security company Cyera. The investments reflect continued investor demand for platforms securing enterprise activity, sensitive information and access by both employees and autonomous AI agents.

EU Cyber Resilience Act Reporting Obligations Take Effect



Manufacturers of products with digital elements must report actively exploited vulnerabilities and severe security incidents through the new single reporting platform. The rules require an early warning within 24 hours and a fuller notification within 72 hours of awareness.

CyberSafe Foundation and SANS Launch AI Security Fellowship for African Women



The fellowship awarded ten African women full access to four AI-security courses and two professional certifications. The programme targets experienced cybersecurity practitioners and seeks to develop specialised capabilities for protecting generative-AI systems and applying AI within security operations.

KEY TRENDS

71%

Infosecurity Magazine

71% of organisations had not conducted an AI-specific incident-response exercise.

4877

CVE Details

4877 CVEs (Common Vulnerabilities and Exposures) created in September 2026.

55.2M

CleanTalk Statistics

CleanTalk Anti-Spam processed approximately 55.2 million spam-related requests during September 2026

1 IN 91

Checkpoint

Approximately one in every 91 enterprise emails was classified as phishing during September

48%

Checkpoint

Global weekly cyberattack volumes increased by 48% year-on-year in September.

320M

Business Standard

Publicly acknowledged data breaches disclosed since September reportedly affected at least 320 million people globally.

CYBER INCIDENT ANALYSIS

Compromised Remote Access → Ransomware-Led Production Disruption

INDUSTRY

- Automotive Components Manufacturing

BRIEF SUMMARY

- A manufacturing company experienced a ransomware attack after attackers gained access through a dormant third-party remote-access account that remained active after completion of a maintenance contract. The attackers used the account to enter the corporate network, obtain elevated privileges and move laterally into production-support systems. Multiple servers were encrypted, including file repositories, production-planning applications and backup-management infrastructure. Manufacturing operations were suspended at two facilities while systems were isolated, investigated and restored from unaffected backups.

ROOT CAUSE ANALYSIS

- A dormant vendor account remained enabled without a defined expiry date.
- Remote access did not require phishing-resistant multi-factor authentication.
- Inadequate segmentation existed between corporate IT and production-support systems
- Excessive privileges enabled access beyond the vendor's original maintenance requiremets
- Backup-management infrastructure was accessible from the production domain.
- Alerts concerning unusual after-hours access were not investigated promptly.

LOSS CATEGORIES TO VICTIM

- Business Interruption, Data Restoration Expenses, Forensic Costs, Loss of Gross Profit, Crisis-Management Expenses

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Coordinated immediate forensic investigation across endpoints, servers and remote-access logs.
- Engaged specialist ransomware negotiators to establish communication and assess the threat actor.
- Appointed restoration specialists to validate backups and prioritise critical production systems
- Engaged legal advisers to assess regulatory, contractual and notification obligations.
- Assisted with quantifying production losses and documenting the business-interruption claim.

LOSS INCURRED

- Production Downtime, System Restoration, Forensic and Legal Costs, Overtime and Expedited-Delivery Expenses

RECOMMENDED PREVENTIVE MEASURES

- Enforce automatic expiry and periodic recertification of all third-party accounts.
- Require phishing-resistant multi-factor authentication for every remote-access connection.
- Segment corporate IT, production-support and operational-technology environments.
- Restrict vendors to approved systems through privileged-access management controls.
- Maintain immutable backups in an isolated security domain with separate credentials.
- Monitor after-hours access, privilege escalation and abnormal administrative activity.

CYBER INCIDENT ANALYSIS

Compromised Supplier Mailbox → Fraudulent Invoice and Payment Diversion

INDUSTRY

- Consumer Goods and Distribution

BRIEF SUMMARY

- A distribution company received an email from the genuine account of a long-standing logistics supplier requesting that pending invoices be paid to an updated bank account. Attackers had compromised the supplier's mailbox, studied previous correspondence and inserted themselves into an active payment discussion. Supporting documents and earlier email threads appeared legitimate, allowing the beneficiary change to bypass informal checks. Several invoices were paid before the supplier reported non-receipt of funds. The company immediately contacted its bank, enabling partial freezing and recovery of the transferred amount.

ROOT CAUSE ANALYSIS

- Beneficiary changes were accepted through email without independent verification.
- Payment staff relied on the familiarity of the supplier's genuine email address and historical thread.
- No mandatory callback was made to a verified supplier contact.
- The finance system did not apply a cooling-off period to newly created beneficiaries.
- Multiple invoices could be released immediately after changing supplier bank details.
- Third-party compromise scenarios were not sufficiently covered in fraud-awareness training.

LOSS CATEGORIES TO VICTIM

- Direct Financial Loss, Fund-Recovery Expenses, Legal Costs, Supplier Dispute and Reputational Impact

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Coordinated forensic review of email headers, payment records and employee devices.
- Engaged legal advisers to assess contractual responsibility between the company and supplier.
- Assisted with evidence preservation and reporting to relevant law-enforcement authorities.
- Assisted with documenting recovered and unrecovered funds for claim assessment.

LOSS INCURRED

- Unrecovered Funds, Forensic and Legal Costs, Fund-Recovery Expenses

RECOMMENDED PREVENTIVE MEASURES

- Require out-of-band verification for every supplier-bank-detail change.
- Use independently maintained contact details rather than information contained in the request.
- Enforce dual approval for new beneficiaries and amended payment instructions.
- Introduce a cooling-off period before payments can be made to newly added accounts.
- Apply transaction-risk scoring based on beneficiary, geography, value and payment timing.
- Train finance teams on compromised-vendor mailboxes and active email-thread hijacking.
- Maintain an immediate-response process involving banks, legal counsel and law enforcement.

ADVISORIES

ADVISORY: PHP2SHELL VULNERABILITIES ENABLE UNAUTHENTICATED REMOTE CODE EXECUTION

- **Cyber Centre Recommendation:** Immediately update affected PHP installations to versions 8.5.12, 8.4.27, 8.3.36 or 8.2.35, restart web services and assess internet-facing systems for possible compromise.
- **Broad Threat Coverage:**
  - CVE-2026-109618 and CVE-2026-109619, collectively called PHP2Shell, are critical vulnerabilities rated CVSS 9.2. They may allow unauthenticated attackers to remotely execute code on vulnerable web servers.
- **Proactive Cybersecurity Measure:**
  - Prioritise internet-facing applications and products with embedded PHP.
  - Upgrade unsupported PHP 8.1 and earlier deployments.
  - Review logs for suspicious processes, file changes, web shells and outbound connections.
  - Enable WAF or IPS protections and isolate systems that cannot be patched immediately.
  - Rotate credentials and secrets if compromise is suspected.

Read more at: CISA PHP2Shell Security Advisory

ADVISORY: CRITICAL CISCO ISE VULNERABILITIES EXPOSE ENTERPRISE IDENTITY AND NETWORK-ACCESS CONTROLS

- **Cyber Centre Recommendation:** Review the deployment and version of Cisco Identity Services Engine and urgently install the applicable fixed releases. Administrators should prioritise externally reachable and high-privilege nodes responsible for authentication and network admission.
- **Broad Threat Coverage:**
  - Identified risks include authentication bypass, remote code execution, command injection and SQL injection.
  - Additional weaknesses could enable session hijacking, information disclosure, path traversal or denial of service.
  - Compromise could undermine centralised identity enforcement, device admission and network-access decisions.
- **Proactive Cybersecurity Measure:**
  - Upgrade all affected Cisco ISE nodes to vendor-confirmed fixed versions.
  - Restrict administrative interfaces to dedicated management networks and authorised administrator workstations.
  - Review recently created accounts, role changes, API activity and unexplained policy modifications.
  - Monitor authentication logs for bypass attempts, unusual RADIUS activity and abnormal administrative API requests.
  - Preserve configuration backups and validate node synchronisation and policy enforcement after remediation.

Read more at: Cisco August 19 Security Advisory Publication

The Cyber Incident Analyses have been created by ICICI Lombard GIC Ltd. and Arete-IR LLP ("Arete"). The Analysis is based on information compiled and analysed from various external sources. The above provided content is only for general knowledge and information purposes only and shall not constitute any legal, financial, professional or any other advice by ICICI Lombard GIC Ltd. and Arete. ICICI Lombard GIC Ltd. and Arete make no representation or warranties, express or implied, regarding the accuracy, completeness or reliability of the information contained herein. ICICI Lombard GIC Ltd. and Arete disclaim any liability for reliance placed by any person(s) upon any advice, opinion, statement, memorandum or other information provided herein and the use of such information shall strictly be at his/her/their sole risk. Arete-IR LLP, LLPIN: AAQ-5318, registered office at Unit 200, Maple Celestia, Plot No. 49, Jayabheri Enclave, Gachibowli, Hyderabad, Telangana - 500032. Arete's trademark belongs exclusively to Arete. ICICI trade logo displayed above belongs to ICICI Bank and is used by ICICI Lombard GIC Ltd. under license and Lombard logo belongs to ICICI Lombard GIC Ltd. ICICI Lombard General Insurance Company Limited, Registered Office: ICICI Lombard House, 414, Veer Savarkar Marg, Prabhadevi, Mumbai – 400025. IRDAI Reg.No.115. Toll Free 1800 2666. Fax No – 022 61961323. CIN (L67200MH2000PLC129408) customersupport@icicilombard.com. www.icicilombard.com ADV/28733.