EDME CYBER PLUGG IN
MONTHLY NEWSLETTER
JAN 2026

JAN ISSUE 11

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 "Pure Extortion" Pivot

Ransomware groups are increasingly abandoning encryption in favor of "pure data extortion". In December, the Qilin group emerged as a leader in this tactic, claiming high-profile victims like the Church of Scientology UK.

MFA is No Longer a Silver

Adversary-in-the-Middle (AiTM) phishing kits that hijack sessions are now used in 75% of Business Email Compromise (BEC) attacks, allowing hackers to bypass standard Multi-Factor Authentication.

India's Unified Security Standard

Under the new Telecom Cyber Security Amendment Rules 2025, digital platforms must now follow the same cybersecurity standards as telecom operators, including mandatory Mobile Number Validation (MNV).

Third-Party & API Weaknesses

Massive data exposures at 700Credit (5.8 million people) and Nissan (21,000 customers) were driven by compromised partner APIs and third-party managed servers (GitLab), highlighting that security is only as strong as the weakest vendor.

Shadow AI Costs

Organizations reported that nearly 1 in 35 GenAI prompts posed a data leakage risk, with breaches caused by "Shadow AI" (unauthorized tools) adding an average of $670,000 to breach costs.

CYBER NEWS

India Records 265M Cyberattacks

A year-end report from Seqrite revealed that India faced over 265 million cyber incidents in 2025. The education, healthcare, and manufacturing sectors were the most targeted, with Maharashtra and Delhi emerging as the hardest-hit regions.

READ MORE >

GPS Spoofing at Major Airports

The Indian government confirmed cyber incidents involving GPS spoofing at seven major airports, including Delhi, Mumbai, and Bengaluru. The attacks disrupted navigation data for aircraft using GPS-based landing, though ATC safeguards prevented operational delays.

READ MORE >

Government Crackdown on SIM Rackets

Delhi Police's IFSO unit dismantled a massive nationwide SIM Box racket in December. The syndicate used illegal devices to route international calls as domestic ones to facilitate large-scale phishing and investment fraud.

READ MORE >

Operational Resilience for Banks

CERT-IN launched a new initiative in December to strengthen the cybersecurity resilience of Indian cooperative banks, aiming to protect digital devices from botnets and AI-driven malware.

READ MORE >

New Audit Guidelines for Critical Infrastructure

CERT-In issued updated Comprehensive Cyber Security Audit Policy Guidelines in late 2025, mandating annual audits for all critical sectors using 231 empanelled security organizations.

READ MORE >

CYBER NEWS

Massive Coupang Data Breach

On December 1, 2025, the South Korean e-commerce giant disclosed a breach exposing the personal information of 33.7 mil. customers. The data included names, mobile numbers, and delivery locations, leading to the resignation of CEO Park Dae-jun.

READ MORE >

Romanian Water Agency Attack

Global ransomware attacks surged 22% year-over-year (YOY), with 727 reported incidents in November. Industrial Manufacturing (12% of victims) emerged as the hardest-hit sector, followed by Business Services. Major groups like Qilin and Clop dominated the threat landscape, increasingly targeting operational technology (OT) systems.

READ MORE >

Nissan Supply Chain Breach

Nissan Fukuoka Sales disclosed that the personal data of 21,000 customers was compromised following a breach at Red Hat. Attackers gained access to a self-managed GitLab instance containing customer management system code.

READ MORE >

Identity Fraud Sophistication Shift

Security reports from December highlighted a global shift in identity fraud toward Deepfake-as-a -Service (DaaS). Attackers are increasingly using high-quality voice and video cloning to bypass corporate authentication in the financial and government sectors.

READ MORE >

University of Phoenix Breach

The Clop ransomware gang exploited a third-party system to access records of 3.5 million individuals, including students and employees. Exposed data included SSNs and dates of birth.

READ MORE >

01
CASE STUDY

Brief Summary:

A commercial printing press suffered a severe loss via **Conversation Hijacking.** After gaining access to a senior manager's account through **credential stuffing,** an attacker remained silent for weeks, monitoring high-value paper supply negotiations. At the invoicing stage, the attacker "corrected" the bank details in an existing email thread, diverting a large-scale payment to a fraudulent account.

Root Cause Analysis:

Lack of Multi-Factor Authentication (MFA):
The initial entry point was a legacy email login that did not require MFA, allowing the attacker to bypass authentication using credentials leaked in a previous third-party data breach.

Absence of E-mail Monitoring Rules:
The attacker created "hidden" inbox rules that automatically moved any replies from the supplier into a "Deleted Items" or archive folder. This allowed the attacker to correspond with the finance department without the account manager ever seeing the incoming warnings or questions.

Process Breakdown in Finance:
The finance team processed the change in banking details based solely on the email's internal "authenticity," failing to follow a mandated out-of-band verification process (like a phone call) for high-value transaction changes.

Loss and Insurance Applicability:

- Direct Financial Defraudment: A significant sum was transferred to a fraudulent offshore account; recovery was impossible as the transfer was only discovered 14 days later during a routine end-of-month reconciliation.
- Contractual Liability: The printing press remained legally obligated to pay the actual supplier for the raw materials, doubling the effective cost of the order and causing a severe liquidity crisis.
- Insurance Limitation: The claim was only partially covered under "social engineering" sub-limits, which were significantly lower than the company's total cyber coverage, as the firm had not documented a "call-back" verification policy for its accounting team.

Recommended Post-Incident Measures:

Mandatory Phishing-Resistant MFA: Deploy hardware security keys or biometric-based authentication across all employee accounts to eliminate the risk of credential-based hijacking.

Implement Out-of-Band (OOB) Verification: Establish a formal policy requiring a voice confirmation via a known, pre-saved phone number for any request to modify banking, wire, or payment instructions.

Automated Inbox Rule Monitoring: Use security tools to alert IT administrators whenever new email forwarding or "delete-on-arrival" rules are created, as these are primary indicators of a compromised account.

Email Authentication Hardening: Fully implement DMARC (Domain-based Message Authentication, Reporting, and Conformance) with a "reject" policy to prevent attackers from spoofing the company's domain for external-facing fraud.

02
CASE STUDY

Brief Summary

In late 2025, a leading South Asian automotive manufacturer disclosed a catastrophic data breach after security researchers discovered that a series of simple cloud misconfigurations had exposed over a lot of sensitive data to the public internet. The leak included customer databases, internal invoices containing personal identification numbers (PAN), and sensitive infrastructure dashboards.

Root Cause Analysis:

Hard-Coded Credentials:
Developers had embedded plaintext AWS access keys directly into the source code of the company's spare-parts portal, allowing anyone with access to the code to authenticate into their cloud environment.

Over-Privileged IAM Roles:
Identity and Access Management (IAM) roles were configured with unrestricted administrative access to all S3 storage buckets, a direct violation of security best practices.

Publicly Accessible Storage:
Multiple S3 buckets were inadvertently set to "Public," making the massive 70 TB dataset accessible to any unauthorized user without a password.

Recommended Post-Incident Measures:

Secrets Management Integration: Implement a dedicated secrets management service (such as AWS Secrets Manager or HashiCorp Vault) to remove hard-coded credentials from source code and automate key rotation.

Automated Exposure Validation: Deploy tools to perform daily exposure validation to ensure that misconfigurations are detected and remediated within hours rather than days.

Strict Adherence to Least Privilege: Audit and restructure all cloud IAM roles to ensure that users and applications are granted only the minimum level of access required for their specific tasks.

Cloud Security Posture Management (CSPM): Adopt a CSPM platform to provide centralized visibility across multi-cloud environments and automatically flag "drift" from secure configuration baselines.

DATA SPOTLIGHT

The Industrialization of AI-Driven Extortion and Identity Fraud

Supporting Statistics:

- AI-Enabled Breach Growth: Approximately 16% of all data breaches in 2025 involved attackers using AI as a core component of their toolkit.
- Shadow AI Risk Exposure: A staggering 99% of organizations have sensitive data dangerously exposed to AI tools, including sanctioned GenAI copilots and unverified "Shadow AI" apps.
- Cost of Unauthorized AI: Organizations reported that breaches caused specifically by "Shadow AI" (unauthorized tools) added an average of $670,000 to the total cost of a data breach in 2025.
- Manufacturing Ransomware Surge: The manufacturing sector experienced a 61% growth in ransomware attacks in 2025, as threat actors shifted focus toward industries where downtime creates maximum financial leverage.
- Third-Party Supply Chain Fallout: The share of breaches traced back to third-party or supplier vulnerabilities doubled in 2025, rising from 15% to roughly 30% of all global incidents.
- Identity Fraud Sophistication: Among data breaches involving AI-driven attacks, 35% utilized deepfake technology to bypass authentication or execute corporate impersonation scams.

Implications and Tactical Risks:

- The "Pure Extortion" Pivot: Ransomware groups are increasingly moving away from simple encryption to "pure data extortion". In December 2025, groups like Clop and Qilin led campaigns targeting sensitive payroll and HR data in core ERP systems (e.g., Oracle EBS) to pressure victims without needing to lock files.
- "Truman Show" Operations: A new trend of "industrialized" investment fraud has emerged where threat actors use AI to create perfectly timed, hyper-personalized voice and video deepfakes to manipulate executives in real-time.
- SaaS Supply Chain Blind Spots: Attackers are exploiting the "implicit trust" between connected SaaS platforms. By compromising a third-party app integrated with tools like Salesforce or SharePoint, they can "island hop" into the environments of thousands of shared customers.

VULNERABILITY WATCH

Microsoft Patch Tuesday December 2025

Microsoft concluded 2025 by addressing 56 vulnerabilities in its December Patch Tuesday update. The release included three Critical and 53 Important vulnerabilities affecting Windows, Office, Exchange Server, and Azure. Notably, the update patched one actively exploited zero-day (CVE-2025-62221) in the Windows Cloud Files Mini Filter Driver, a use-after-free flaw that allows local attackers to elevate privileges to the SYSTEM level. Additionally, two publicly disclosed vulnerabilities were addressed: a remote code execution (RCE) flaw in GitHub Copilot for JetBrains (CVE-2025-64671) and another RCE in PowerShell (CVE-2025-54100).

Adobe Patches for December 2025

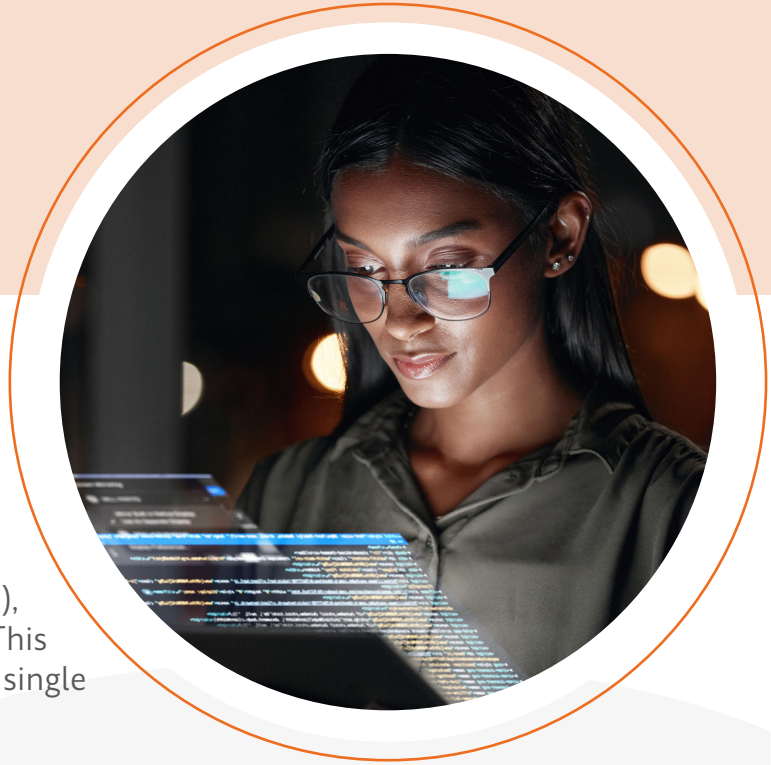
Adobe released five security bulletins in December 2025, resolving a total of 142 vulnerabilities. While most updates were rated as Priority Three, the Adobe ColdFusion update (APSB25-105) was designated Priority One, addressing the bulk of the month's flaws, including risks of remote code execution and data manipulation. Critical updates were also issued for Adobe Acrobat and Reader (APSB25-119), fixing vulnerabilities that could lead to arbitrary code execution and security feature bypasses. Users were also warned of an actively exploited critical flaw in Adobe Commerce and Magento (CVE-2025-54236) earlier in the quarter, requiring immediate hotfixes.

Google Chrome Security Updates November 2025

Google released an urgent emergency update for Chrome in December 2025 to address its eighth zero-day vulnerability of the year. Tracked via an internal reference (ID 466192044) and later coordinated as a high-severity flaw, the vulnerability was confirmed to be exploited in the wild. The update to Chrome version 143 also resolved two medium-severity vulnerabilities: a use-after-free issue in the Password Manager (CVE-2025-14372) and a flaw in the Chrome Toolbar. Due to the active exploitation of the unnamed zero-day, Google initially restricted technical details to ensure the majority of users could patch their systems first.

SECURITY ADVISORIES

Key Recommendations to Protect Your Business



Zero Trust Architecture for Third-Party Ecosystems

The primary defense challenge is the erosion of the traditional network perimeter due to sprawling third-party and vendor integrations. Organizations must adopt a strict Zero Trust model that mandates "never trust, always verify" for every external connection. By enforcing Multi-Factor Authentication (MFA) and the Principle of Least Privilege (PoLP), businesses can ensure that vendors only access the specific data required for their role. This granular control is essential to limit the "blast radius" of a potential breach, preventing a single compromised partner from gaining lateral access to your core network.

Software Supply Chain Transparency via SBOMs

To mitigate systemic risks from open-source and proprietary code, organizations should mandate the use of Software Bill of Materials (SBOMs). These machine-readable "ingredient lists" provide comprehensive visibility into all code dependencies, allowing security teams to rapidly identify and remediate zero-day vulnerabilities (such as Log4j-style flaws) before they can be exploited. Integrating SBOMs with Software Composition Analysis (SCA) tools ensures continuous monitoring of the supply chain, enabling an automated and proactive defense against cascading disruptions.

CYBER QUIZ

FIND ANSWERS IN
THE NEXT EDITION

Which of the following is the most effective way to verify a request to change a vendor's banking details received via email?

A. Reply to the email asking the sender to confirm the new details are correct.
B. Check the email headers to ensure the sender's IP address matches their known location.
C. Use an "out-of-band" method, such as calling a known, trusted phone number for that vendor.
D. Compare the digital signature in the email against a previous invoice from the same vendor.

What is the primary purpose of Cloud Security Posture Management (CSPM) tools?

A. To provide faster internet speeds for remote workers using cloud applications.
B. To continuously monitor cloud environments for misconfigurations, such as publicly exposed data buckets.
C. To act as a digital vault for storing an organization's administrative passwords.
D. To automatically generate marketing content using generative AI based on stored cloud data.

ANSWERS FOR DECEMBER CYBER PLUGGED-IN NEWSLETTER QUIZ

Ans: **D** It ensures that a compromised password alone is insufficient to grant unauthorized access.

Ans: **C** Maintaining isolated (air-gapped or immutable) backups of all critical data.

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**