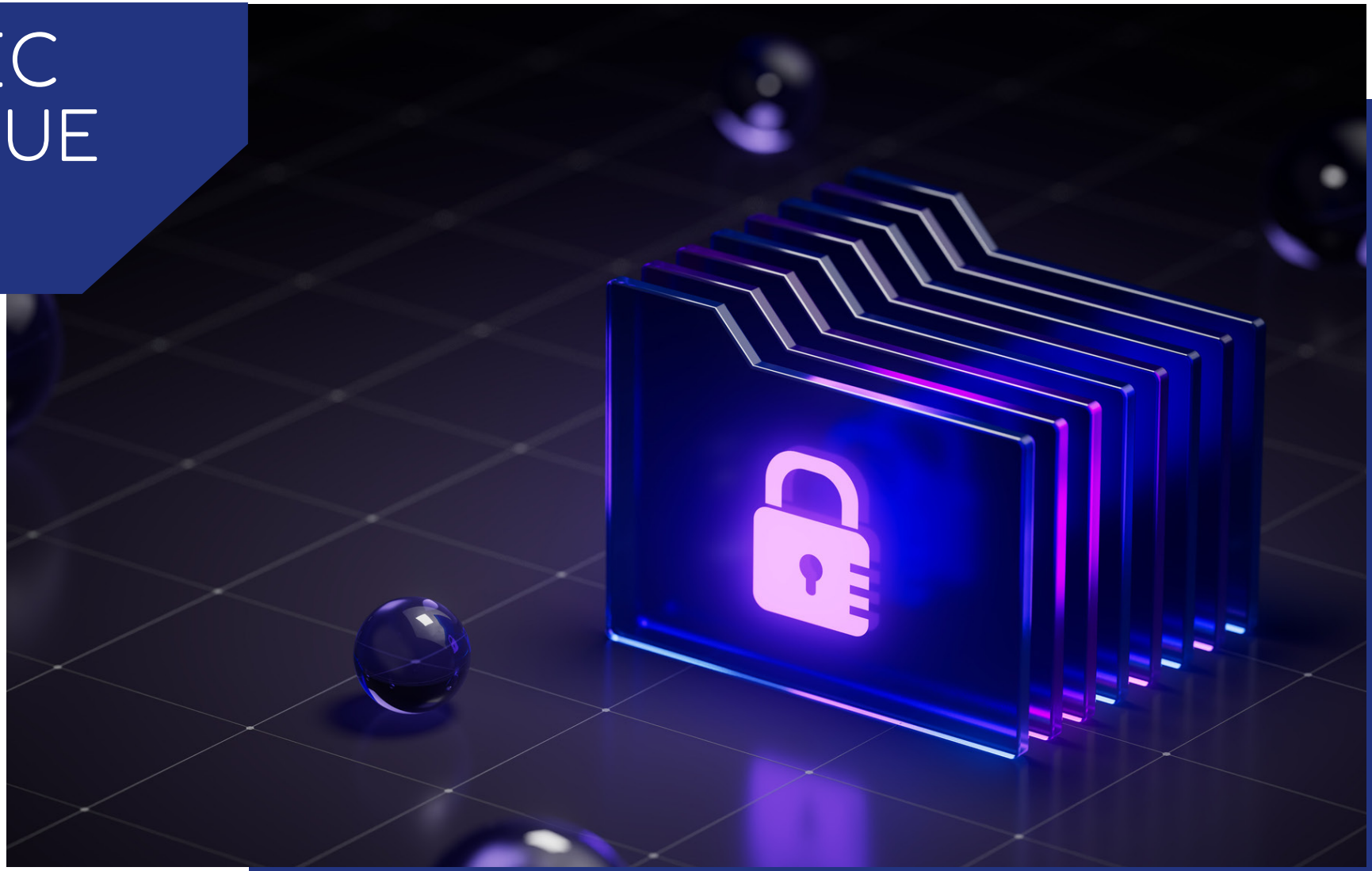
EDME CYBER PLUGG IN
MONTHLY NEWSLETTER
DEC 2025

DEC ISSUE 10



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

GenAI Risks Intensify: Hyper-personalized Ransomware and Data Leakage

The use of Generative AI (GenAI) by threat actors has scaled, leading to a 22% Year-over-Year increase in global ransomware attacks in November. New AI-driven ransomware delivers hyper-personalized, human-like phishing and autonomously adapts attack tactics. Furthermore, the rapid adoption of GenAI tools within organizations introduced significant data-exposure risks, with reports showing that approximately 1 in every 35 GenAI prompts carried a high risk of sensitive data leakage.

Sophistication Shift in Identity Fraud and Deepfake-as-a-Service (DaaS)

The focus of identity fraud has shifted from high-volume attempts to fewer, but more damaging, sophisticated attacks. The rise of Deepfake-as-a-Service (DaaS) platforms on the dark web has made voice and video cloning easily accessible, fueling an increase in synthetic identity use and highly convincing corporate impersonation scams, particularly targeting financial and government sectors.

Critical Vulnerability Exploitation and Supply Chain Fallout

November saw the final stages of large-scale data-theft operations, notably by the Clop ransomware group, which exploited zero-day vulnerabilities in enterprise software like Oracle E-Business Suite. This highlighted the persistent danger of unpatched systems and the continued fallout from supply-chain breaches where attackers leverage third-party vendor access for initial compromise.

Targeting of Operational Technology (OT) and AI Model Pipelines

Industrial Manufacturing emerged as the hardest-hit sector globally for ransomware. Attackers are increasingly exploiting operational dependencies and legacy systems in OT environments. A new vector emerged with the targeting of AI Model Training Pipelines—where adversaries inject poisoned datasets to manipulate model outputs or introduce exploitable backdoors in critical systems like fraud detection engines.

CYBER NEWS

DPDP Rules Operationalized: New Era for Data Protection

The Ministry of Electronics and Information Technology (MeitY) officially notified the Digital Personal Data Protection (DPDP) Rules, 2025 on November 14. This fully operationalizes the DPDP Act 2023, introducing strict compliance obligations for businesses (Data Fiduciaries). Key requirements include mandatory 72-hour breach reporting to the Data Protection Board (DPB) and a requirement for annual security audits for Significant Data Fiduciaries.

READ MORE >

CERT-In Issues High-Severity Alert for Google Chrome

The Indian Computer Emergency Response Team (CERT-In) released a high-severity advisory urging all users to update Google Chrome immediately. The warning highlighted multiple vulnerabilities, including in the V8 JavaScript engine, that could allow remote attackers to execute arbitrary code and gain full control of affected systems simply by tricking users into visiting a malicious website.

READ MORE >

Indian Companies Rank Cyber Threats as Top Risk for 2025

A major global risk management survey (AON's 2025 Global Risk Management) released its findings in November, revealing that "Cyber Attacks and Data Breach" remained the top risk agenda for most Indian companies. This sentiment was closely followed by concerns over "Data Privacy Requirements/Non-Compliance," reflecting the heightened awareness due to new regulatory frameworks like DPDP.

READ MORE >

Surge in AI-Driven Ransomware and Data Leakage Risks

Reports from the threat intelligence community noted a global surge in ransomware activity, with India being heavily impacted. The trend is driven by AI-assisted espionage and threat actors leveraging Generative AI (GenAI) to create hyper-personalized phishing attacks. Furthermore, the widespread adoption of GenAI tools within Indian enterprises introduced a new risk, with up to 1 in 35 GenAI prompts carrying a high risk of sensitive data leakage from corporate systems.

READ MORE >

Telecom Sector Measures Against Fraud and SIM Swapping

The Department of Telecommunications (DoT) issued new directions aimed at securing the mobile ecosystem and reducing financial fraud. These included mandates for mobile handset manufacturers to pre-install the 'Sanchar Saathi' App to allow citizens to verify the authenticity of devices via their IMEI number, directly combating the use of stolen or spoofed devices in SIM swap and UPI phishing scams.

READ MORE >

CYBER NEWS

GenAI Fuels Attack Sophistication and Data Leakage

Generative AI (GenAI) is accelerating attacks, creating hyper-personalized phishing and automating full breach cycles (e.g., Anthropic's disclosure of an AI-assisted espionage campaign). Crucially, enterprise use of GenAI is a major risk, with research finding that 1 in 35 prompts from corporate networks carried a high risk of sensitive data leakage.

READ MORE >

Ransomware Surge Hits Manufacturing Hardest

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 >

Zero-Day Exploits Create Global Supply Chain Fallout

The ripple effect of supply chain attacks intensified. The Clop ransomware group successfully exploited zero-day vulnerabilities in Oracle E-Business Suite, leading to massive data breaches at numerous global firms (including Hitachi-owned GlobalLogic and The Washington Post), confirming the immense risk of single-point vendor compromises.

READ MORE >

Critical Vulnerability Exploits Force Rapid Patching

The U.S. CISA was forced to issue a directive requiring federal agencies to immediately patch a critical, actively exploited Remote Code Execution (RCE) vulnerability in Fortinet products. This was the seventh Fortinet flaw in CISA's Known Exploited Vulnerabilities catalog for 2025, highlighting the continuous pressure on network infrastructure security.

READ MORE >

Education Sector Remains Top Target Worldwide

Despite heightened focus on critical infrastructure, the Education sector remained the most frequently attacked globally, averaging 4,656 attacks per organization per week (+7% YOY). This confirms the continuous value of their data and the vulnerability of their typically decentralized, under-resourced networks to financial and espionage motives.

READ MORE >

01
CASE STUDY

Brief Summary:

A mid-sized regional healthcare provider was targeted by the "MedLocker" ransomware strain, which resulted in the encryption of critical patient records (EHRs), appointment scheduling systems, and internal communication platforms. The attack was initiated through a successful exploit of an unpatched vulnerability in an obsolete Remote Desktop Service (RDP) on a peripheral server. The attackers demanded a ransom of $500,000 in Monero. The resulting system downtime forced the cancellation of all non-essential procedures and diverted emergency patients for over a week.

Root Cause Analysis:

Phishing and Social Engineering:
Targeted spear-phishing emails successfully harvested login credentials of key finance personnel.

Lack of Multi-Factor Authentication (MFA):
The compromised email account did not enforce MFA, allowing attackers to access it with stolen credentials.

Inadequate Transaction Controls:
Absence of dual-approval processes for large payments enabled fraudulent wire transfers without verification.

Loss and Insurance Applicability:

- Financial loss of $3 million due to unauthorized transfers, along with forensic investigation and legal fees.
- Reputational harm and loss of client trust adversely impacted business opportunities.
- Cyber insurance partially covered investigation and recovery costs, but coverage for payment fraud was limited as no advanced email security protocols were documented.

Recommended Post-Incident Measures:

Implement mandatory multi-factor authentication on all email accounts.

Establish dual-approval workflows for outbound wire transfers exceeding defined thresholds.

Deploy advanced email filtering and phishing detection solutions with employee awareness training.

Conduct regular internal audits of financial transaction processes and incident response drills.

02
CASE STUDY

Brief Summary

A financial services firm suffered a major data breach when a developer accidentally left an Amazon S3 bucket hosting client investment documents publicly accessible. The misconfiguration was identified by a security researcher and subsequently scraped by a threat actor before it could be secured. The exposed data included millions of records containing Personally Identifiable Information (PII) and sensitive financial statements for clients across four countries. The bucket was exposed for 48 hours.

Root Cause Analysis:

Misconfiguration Error:
A developer, while troubleshooting a third-party integration, mistakenly set the S3 bucket policy to 'Public Read/Write' instead of using a restricted IAM role, bypassing security checks.

Lack of Automated Cloud Security Posture Management (CSPM):
The organization did not have real-time monitoring tools to automatically detect and alert on public-facing storage resource configurations.

Overly Permissive Access:
The developer role itself had excessively broad permissions to change S3 bucket settings, enabling the error to occur.

Recommended Post-Incident Measures:

Implement a Cloud Security Posture Management (CSPM) solution for continuous, automated monitoring and remediation of public misconfigurations.

Enforce the Principle of Least Privilege (PoLP) across all cloud Identity and Access Management (IAM) roles, especially for developers and non-production accounts.

Implement Guardrails and Automated Prevention: Use cloud-native tools (like AWS Config Rules or Azure Policy) to automatically deny or revert storage buckets if they are set to 'Public Access.'

Conduct mandatory, annual Secure Cloud Configuration Training for all engineering and development staff.

DATA SPOTLIGHT

Geopolitical Cyber Warfare and Critical Infrastructure Targeting

Supporting Statistics:

- Geopolitical Influence on Cyber Strategy: Nearly 60% of organizations reported that escalating geopolitical tensions directly influence their cybersecurity strategy and spending decisions (Source: WEF Global Cybersecurity Outlook, 2025).
- CEO Concerns Shift: 45% of cyber leaders and a third of CEOs cite disruption of operations and business processes as their top cyber concern, reflecting the shift from data theft to physical sabotage (Source: WEF Global Cybersecurity Outlook, 2025).
- Critical Infrastructure Preparedness Confidence Gap: Only 15% of organizations in Europe and North America lack confidence in their country's CI preparedness, but this figure surges to 42% in Latin America and 36% in Africa, highlighting a severe cyber inequity (Source: WEF Global Cybersecurity Outlook, 2025).
- Manufacturing Hit Hardest by Ransomware: Industrial Manufacturing was the most victimized sector globally in November, accounting for 12% of all disclosed ransomware incidents, due to reliance on vulnerable Operational Technology (OT) and critical supply chains (Source: Check Point Research, Nov 2025).
- Surge in ICS Vulnerability Disclosures: CISA released multiple advisories in November, contributing to a total of 2,065 new CVEs (Common Vulnerabilities and Exposures) disclosed in Industrial Control Systems (ICS) products in 2025, the highest on record (Source: CISA/SOCRadar, 2025).
- Compromised Access Market Activity: There were 3,013 incidents related to the sale of compromised network access on cybercrime forums in 2025, demonstrating the ease with which initial access to high-value targets is monetized (Source: Cyble Global Threat Report, 2025).

Implications and Tactical Risks:

- Conflict Spillover: Nation-state cyber activity, initially aimed at government targets, is increasingly spilling over to disrupt private sector critical infrastructure and supply chains as collateral damage.
- OT/ICS Vulnerability: The high volume of vulnerabilities in ICS devices, coupled with the complexity of patching safety-critical industrial systems, makes them prime targets for disruptive attacks.
- Undersea Cables and Satellites: Attacks on global communications infrastructure, including undersea cables and satellites, are a growing geopolitical tactic, threatening global data flow and economic stability.

VULNERABILITY WATCH

Microsoft Patch Tuesday November 2025

Microsoft released patches addressing a total of 63 vulnerabilities in its November 2025 Patch Tuesday update. Among these, five were rated Critical, including a high-severity Remote Code Execution (RCE) flaw in the Microsoft Graphics Component (GDI+) with a CVSS score of 9.8, and another RCE in Microsoft Office. Crucially, one actively exploited zero-day vulnerability was patched in the Windows Kernel (CVE-2025-62215) that could allow a local, authenticated attacker to elevate their privileges to the SYSTEM level. The majority of fixes addressed Elevation of Privilege and Remote Code Execution risks, underscoring the urgent need for organizations to prioritize deployment, especially for the exploited kernel flaw.

Adobe Patches for November 2025

Adobe released eight security advisories addressing a total of 29 vulnerabilities in its November 2025 updates, affecting products including Adobe InDesign, InCopy, Photoshop, Illustrator, Substance 3D Stager, and Format Plugins. Of these, 23 vulnerabilities were rated Critical, the majority of which could lead to arbitrary code execution through successful exploitation of flaws like Heap-based Buffer Overflows and Use After Free. Immediate updates are recommended for all Creative Cloud users, as these critical flaws pose a severe risk of system compromise, particularly within design and media-focused enterprises.

Google Chrome Security Updates November 2025

Google released an urgent, out-of-band security update in November 2025, addressing five critical vulnerabilities. The most serious was a confirmed actively exploited zero-day (CVE-2025-13223), a high-severity Type Confusion flaw in the V8 JavaScript engine. This vulnerability allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, leading to arbitrary code execution. Users were strongly advised to update to Chrome version 142.0.7444.175 or later on all desktop and mobile platforms to immediately protect against ongoing exploit campaigns.

SECURITY ADVISORIES

Key Recommendations to Protect Your Business

Cloud Security Posture Management (CSPM)

The primary defense challenge in November is driven by the convergence of cloud security risks and systemic supply chain vulnerabilities. Organizations must prioritize Cloud Security Posture Management (CSPM) to continuously monitor and automatically correct misconfigurations such as publicly exposed storage and overly permissive access which are the leading cause of cloud breaches and ransomware infiltration. Crucially, strict AI Data Governance is required to prevent employees from leaking sensitive corporate information via popular Generative AI tools, a high-frequency risk observed across enterprises this month.

Zero Trust model

To mitigate systemic threats, focus on Software Supply Chain and Third-Party Risk. Mandate comprehensive visibility through the use of Software Bill of Materials (SBOMs) for all code dependencies, enabling rapid response to zero-day vulnerabilities in common components. Simultaneously, treat all vendor and third-party connections as high-risk by enforcing a strict Zero Trust model with MFA and the Principle of Least Privilege, ensuring that a compromise at a single vendor does not lead to a catastrophic breach of your core network.

CYBER QUIZ

FIND ANSWERS IN
THE NEXT EDITION

What is the primary benefit of enabling Multi-Factor Authentication

A. It encrypts all the user's files and documents in the cloud.
B. It automatically updates the user's password every 30 days.
C. It prevents all spam and phishing emails from reaching the user's inbox.
D. It ensures that a compromised password alone is insufficient to grant unauthorized access.

Which security measure is considered the most critical last line of defense against a successful ransomware attack?

A. Mandatory bi-weekly password changes for all system administrators.
B. Strictly limiting employee access to only necessary network segments (least privilege).
C. Maintaining isolated (air-gapped or immutable) backups of all critical data.
D. Using advanced, real-time antivirus and Endpoint Detection and Response (EDR) software.

ANSWERS FOR NOVEMBER CYBER PLUGGED-IN NEWSLETTER QUIZ

Ans: **C** To control incoming and outgoing network traffic based on security rules

Ans: **A** Receiving unexpected emails with urgent requests for personal information

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

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.

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**