EDME CYBER PLUGG IN
MONTHLY NEWSLETTER
OCT 2025

OCT ISSUE 08

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

Rise of AI-Driven Ransomware and Prompt-Based Attacks

AI is now used not just for social engineering, but as the foundation for attacks, prompt-based ransomware like "PromptLock" showcases autonomous, self-adapting malware capable of double extortion and automated decision-making in targeting and evasion. These attacks are harder to defend against using traditional signature-based tools.

SaaS Supply Chain and OAuth Attacks

September saw multiple SaaS supply chain incidents, with OAuth token abuse in platforms like Salesloft and Drift, and Microsoft tightening domains to reduce phishing and spam vectors. Legacy software vulnerabilities (e.g., WinRAR zero-days) were again widely exploited, and there was a trend toward exploiting cloud and SaaS interconnections for lateral movement.

Shadow AI and Synthetic Identity Fraud

“Shadow AI” : the unauthorized use of AI tools and models has become a critical risk, alongside synthetic identity fraud that leverages stolen data and generative AI to make detection difficult. These trends are expected to dominate the threat landscape heading into Q4.

Critical Sector Targeting & Data Breaches

Large-scale attacks continued targeting healthcare, telecom, and government systems worldwide. High-profile data breaches included the theft of millions of customer records from automotive brands, exploitation of power sector vulnerabilities, and new regulations specifically for power infrastructure cybersecurity in India.

Surge in Large-Scale Financial and SIM Fraud

In India, a marked uptick in financial cyber fraud involving UPI phishing, SIM card abuse, and large-scale mobile identity attacks was reported. The government responded by deactivating fraudulent accounts and SIMs, and increasing the budget for national cybersecurity initiatives.

CYBER NEWS

India's Cybersecurity Administration and Telecom Security

India remains the second most targeted country worldwide for cyberattacks, facing rising ransomware, phishing, and supply chain attacks. The government strengthened telecom cybersecurity with new rules mandating rapid breach notification, data sharing, and appointment of chief security officers in telecom companies to safeguard critical infrastructure..

READ MORE >

Evolving Cybersecurity Laws in India

India implemented major legislative reforms replacing colonial-era codes with three new laws in 2023-2024, integrating cybercrimes into mainstream criminal laws with harsher penalties. Recent draft telecom cybersecurity rules expanded monitoring and reporting obligations, while CERT-In updated vulnerability reporting guidelines to strengthen national cyber defenses.

READ MORE >

Data Breach Statistics and Impact

India witnessed a surge in data breaches, ranking fifth globally in breached accounts with 5.3 million compromised in 2023. Phishing was the most prevalent attack vector, causing 22% of incidents, followed by credential compromise. The average cost of a data breach in India reached $2.18 million, highlighting the urgent need for improved cybersecurity frameworks.

READ MORE >

Surge in Cyberattacks Against Education Sector

With schools reopening, cyberattacks targeting educational institutions surged in September, exploiting vulnerabilities in online learning platforms. The surge forced a reevaluation of cybersecurity measures in the sector, while AI technologies were increasingly deployed to fill gaps amid shrinking cybersecurity budgets.

READ MORE >

National Cyber Coordination and Key Arrests

September saw key developments in national cyber coordination with Navin Kumar Singh appointed as the fourth National Cybersecurity Coordinator, marking a significant leadership transition. Law enforcement agencies arrested several cybercriminals involved in multi-crore credit card frauds and insider data theft across various states. Additionally, a cyber breach of West Bengal Police's cybercrime data center raised concerns about data integrity and vendor accountability.

READ MORE >

CYBER NEWS

Ransomware and Malware Activity

The ransomware threat landscape remained intense, with 504 global ransomware victims reported in September. Key players included the Akira ransomware group, responsible for nearly 40% of attacks, and new entrants such as Dire Wolf, Coinbase Cartel, and Lunalock focusing on data theft, extortion, 1GVC widespread encryption. Emerging groups deployed stealthy delivery mechanisms & expanded operations into new environments including Linux. Extortion-only groups like World Leaks and PEAR Team increased activity, exfiltrating massive data volumes.

READ MORE >

Major Data Breaches

Several high-impact data breaches were reported globally. A colossal breach exposed 16 billion passwords and credentials across multiple platforms, including Facebook, Google, Apple, Telegram, and GitHub, primarily from infostealer malware. Another breach impacted a covert U.S. government communication app, exposing unencrypted messages and sensitive personnel information. Prominent companies, including luxury retail & airline sectors, also suffered breaches leading to compromised customer and employee data.

READ MORE >

State-Backed Cyber Espionage

State-sponsored cyber espionage surged particularly in East Asia, North America, and Southeast Asia. Chinese hackers targeted government and industrial sectors, increasing attacks by up to 150% compared to previous periods. North Korean operatives extended espionage operations into Europe and Asia, employing novel backdoors and command-control mechanisms. Campaigns such as “Salt Typhoon” amassing global surveillance data also gained attention. Attacks frequently exploited zero-day vulnerabilities and supply chain weaknesses.

READ MORE >

Critical Infrastructure and Election Attacks

A major DDoS campaign targeted Moldova’s September 2025 parliamentary elections, with over 14 million attack attempts aimed at electoral systems, government websites, and overseas voting stations. Attackers hijacked domestic home routers to create botnets facilitating large-scale disruption, signaling possible nation-state involvement. European airports experienced ransomware-induced flight delays, and new world records in DDoS defenses were also noted.

READ MORE >

AI-Driven Cybercrime Trends

Artificial intelligence continued to amplify cybercrime capabilities, aiding threat actors in precision-guided DDoS attacks, ransomware evolution, and sophisticated phishing schemes. AI-powered ransomware-as-a-service emerged, blending nation-state and criminal tactics. The G7 cyber expert group called for coordinated efforts to manage AI cybersecurity risks amid escalating threats.

READ MORE >

01
CASE STUDY

Brief Summary:

A global financial services firm experienced a data breach after attackers exploited vulnerabilities in its third-party vendor's API integration. The exposed interface allowed unauthorized requests that retrieved sensitive transaction and client data, including account details and investment portfolios. The breach remained undetected for nearly a month, resulting in large-scale data leakage and potential insider trading risks.

Root Cause Analysis:

Insecure API Configuration:
The vendor's API lacked proper authentication and rate-limiting controls, permitting unauthorized access through exploited tokens.

Vendor Oversight Failure:
The financial firm did not conduct periodic security assessments or enforce contractual security requirements with its third-party vendors.

Limited Monitoring:
Logs from the API environment were not integrated into the enterprise SIEM, delaying anomaly detection and incident response.

Loss and Insurance Applicability:

- Exposure of client and financial transaction data led to potential legal liabilities, insider trading investigations, and regulatory compliance actions.
- The company suffered significant financial loss due to market manipulation risks, client churn, and forensic investigation costs.
- Cyber insurance partially covered third-party related incidents, but coverage was limited since vendor audits and API monitoring controls were not documented before the breach.

Recommended Post-Incident Measures:

Implement continuous third-party risk management, including automated API security scanning and contractual compliance checks.

Enforce strict access tokens, mutual authentication, and payload validation for all API traffic.

Integrate third-party monitoring into the central SIEM and establish incident response playbooks for vendor-related incidents.

Conduct periodic audits of vendor security posture and contractually mandate compliance with enterprise security policies.

02
CASE STUDY

Brief Summary

A regional manufacturing company suffered a ransomware attack delivered through a compromised Remote Desktop Protocol (RDP) service. Attackers leveraged weak passwords and unpatched systems to gain entry, then deployed a double-extortion ransomware variant that both encrypted operational data and exfiltrated intellectual property (design blueprints and prototypes). Production lines were halted for days, resulting in operational downtime and shipment delays.

Root Cause Analysis:

Weak Endpoint Security:
RDP servers were exposed to the internet with basic password authentication and no multi-factor protection.

Unpatched Vulnerabilities:
Several endpoints ran outdated OS versions lacking critical ransomware protection updates.

Lack of Network Isolation:
Operational Technology (OT) and IT environments shared the same network, making lateral movement easy during the attack.

Loss and Insurance Applicability:

- The attack disrupted manufacturing operations for nearly a week, leading to loss of revenue, missed client deliveries, and exposure of proprietary designs.
- Costs were incurred for system decryption, forensic restoration, and reputational damage management.
- Insurance covered data recovery and forensic expenses but excluded ransom payment and losses related to intellectual property theft.

Recommended Post-Incident Measures:

Implement multi-factor authentication and network-level RDP gateway controls with restricted IP allowlists.

Enforce an OT- IT segmentation model with strict firewall policies to prevent lateral spread.

Deploy EDR solutions and establish baseline configurations with automated patching policies.

Maintain offline backups of critical production and design systems, and test restoration under simulated ransomware scenarios.

Revise insurance policies to ensure adequate coverage for IP-related losses and business downtime.

DATA SPOTLIGHT

- India recorded its highest-ever average cost of a data breach at INR 220 million (USD 2.65 million) — a 13% increase year-on-year, even as the global average declined by 9% to USD 4.44 million. This surge underscores the growing financial impact of cyber incidents in the region, especially as organizations rapidly adopt AI technologies without robust governance and security controls.

- Recovery timelines remain a major concern, with breaches in hybrid environments taking an average of 276 days to resolve and costing up to USD 5.05 million. The prolonged disruption not only inflates direct costs but also amplifies reputational and regulatory risks.

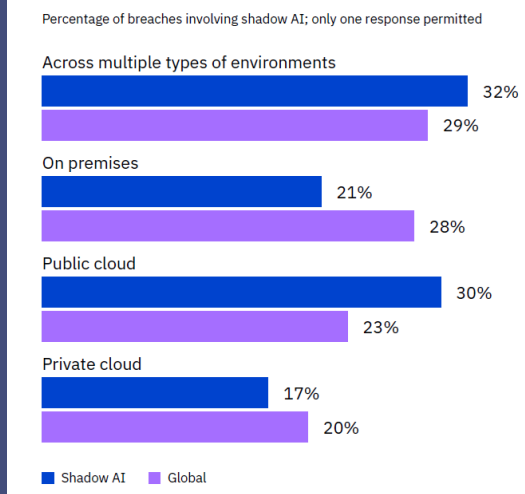
- AI is increasingly shaping the threat landscape. 13% of breaches involved an AI model or application, and 97% of organizations reported inadequate AI access controls. Attackers are weaponizing AI too — 37% of AI-enabled attacks use phishing, while 35% involve deepfakes. The rise of shadow AI, found in 20% of breaches, adds further complexity, increasing breach costs by an average of USD 200,000, and up to USD 670,000 in high-use environments.

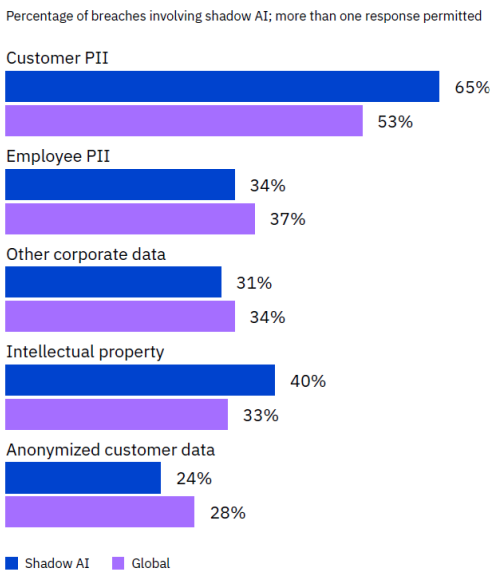
- The most common target remains customer PII (53%), but intellectual property losses are the most expensive. Regulatory scrutiny is intensifying, with 32% of incidents triggering fines, nearly half exceeding USD 100,000.

Measured in USD millions

#	Country		2025	2024
1	United States	↑	$10.22	$9.36
2	Middle East	↓	$7.29	$8.75
3	Benelux	↑	$6.24	$5.90
4	Canada	↑	$4.84	$4.66
5	United Kingdom	↓	$4.14	$4.53
6	Germany	↓	$4.03	$5.31
7	Latin America	↓	$3.81	$4.16
8	France	↓	$3.73	$4.17

#	Country		2025	2024
9	ASEAN	↑	$3.67	$3.23
10	Japan	↓	$3.65	$4.19
11	Italy	↓	$3.44	$4.73
12	South Korea	↓	$2.84	$3.62
13	Australia	↓	$2.55	$2.78
14	India	↑	$2.51	$2.35
15	South Africa	↓	$2.37	$2.78
16	Brazil	↓	$1.22	$1.36





DATA SPOTLIGHT

AI Threats and Supply Chain Exposure Surge in September 2025

- AI-powered cyberattacks have become more autonomous and stealthy, with attackers using adaptive malware that evades detection by changing behavior dynamically (Source: Cybervizer, Sept 2025).
- Phishing attacks are increasingly hyper-personalized through generative AI, leveraging public and private data to craft convincing lures (Source: Cybervizer, Sept 2025).
- Autonomous AI agents are actively probing networks for vulnerabilities without human guidance, raising threat sophistication (Source: Cybervizer, Sept 2025).
- Supply chain cyber risks expanded beyond software to include hardware firmware vulnerabilities, with attackers exploiting weaknesses in component sourcing and firmware update processes (Source: Cybervizer, Sept 2025).
- Investment in AI-driven cybersecurity continues, with 82% of IT decision-makers planning increased spending on AI-based defense solutions within two years (Source: Lakera AI Security Report, Sept 2025).
- Despite AI adoption, only 5% of organizations feel highly confident in their AI security preparedness, signaling a critical need for improved governance and training (Source: Lakera AI Security Report, Sept 2025).

Implications and Tactical Risks:

- AI is a double-edged sword in cybersecurity, enhancing both defender capabilities for real-time detection and response, and attacker sophistication via AI-generated malware and social engineering attacks.
- Supply chain exposures are increasingly complex, requiring comprehensive visibility into hardware and firmware provenance alongside software vigilance.
- Organizations must embrace AI-driven security solutions, human expertise, and strong governance frameworks to mitigate evolving AI-powered threats and secure increasingly intricate supply chains.

VULNERABILITY WATCH

Microsoft Patch Tuesday September 2025

Microsoft addressed a total of 86 vulnerabilities in its September 2025 Patch Tuesday release. Among these, 9 were rated Critical, including 5 Remote Code Execution (RCE) flaws impacting Windows Kernel, NTLM, Graphics components, Hyper-V, and Microsoft Office. Two zero-day vulnerabilities were publicly disclosed and patched: a Windows SMB Elevation of Privilege (CVE-2025-55234) and a Denial of Service vulnerability in Newtonsoft.Json used by SQL Server. Organizations are urged to prioritize patching due to the severity and active disclosure of some flaws.

Adobe Patches for September 2025

Adobe fixed 22 vulnerabilities across multiple products including Acrobat Reader, After Effects, Premiere Pro, Adobe Commerce, and ColdFusion. Out of these, 12 were rated critical, addressing critical risks such as arbitrary code execution and security feature bypass. Immediate application of updates is recommended to mitigate risks.

Google Chrome Security Updates September 2025

Google released security updates addressing four vulnerabilities, including an actively exploited zero-day in the V8 JavaScript and WebAssembly engine (CVE-2025-10585) causing type confusion and potential remote code execution. Users are advised to update to Chrome version 140.0.7339.185 or later on all platforms to defend against active exploits.

SECURITY ADVISORIES

Key Recommendations to Protect Your Business

Bolster Endpoint Security Against Emerging Malware and Ransomware Threats

The sophistication of modern ransomware and malware campaigns continues to grow, often exploiting zero-day vulnerabilities and leveraging fileless attack techniques to evade detection. Organizations should implement robust endpoint detection and response (EDR) solutions capable of real-time threat hunting and behavior analysis. Regular patching, application whitelisting, and network segmentation further help contain potential outbreaks. Conducting threat simulations and maintaining offline, immutable backups are critical steps to ensure resilience and minimize downtime during potential ransomware incidents.

Improve Identity and Access Management (IAM) to Prevent Unauthorized Access

Compromised credentials remain a primary entry vector for attackers targeting corporate systems and cloud environments. To strengthen identity defense, businesses should enforce Multi-factor Authentication (MFA) across all critical applications, adopt passwordless or risk-based authentication mechanisms, and practice Just-In-Time (JIT) access provisioning. Implementing centralized IAM with continuous access review and logging can reduce insider threats and ensure traceability. Periodic access audits and strict enforcement of least-privilege principles significantly reduce the risk of unauthorized data exposure.

CYBER QUIZ

FIND ANSWERS IN
THE NEXT EDITION

Which of the following techniques is commonly used to evade detection in Advanced Persistent Threat (APT) attacks?

A) Using polymorphic malware that continuously changes its code to avoid signature-based detection.
B) Flooding the target network with malicious traffic to cause denial of service.
C) Sending phishing emails with obvious spelling errors to filter out unalerted victims.
D) Using ransomware that immediately announces itself to the victim.

In zero-trust security architecture, what is the primary principle applied to user and device access?

A) Assume all users inside the network are trusted and grant full access by default.
B) Continuously verify and enforce least-privilege access based on user identity, device health, and context.
C) Only require password authentication once per session and trust the device thereafter.
D) Use a single firewall to block all traffic from outside the corporate network.

ANSWERS FOR OCTOBER CYBER PLUGGED-IN NEWSLETTER QUIZ

Ans: **A** An attacker injects malicious scripts into a trusted website that run in users' browsers, potentially stealing session tokens or manipulating content.

Ans: **B** Attackers manipulate the training data or inputs of machine learning models to cause them to misclassify or malfunction.

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**