EDME CYBER PLUGG IN MONTHLY NEWSLETTER

NOV 2025

NOV
ISSUE
09

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

Expansion of AI-Enabled Cyberattacks and Threat Automation

AI-powered attacks continue to evolve, with threat actors deploying autonomous malware capable of adapting tactics in real time. New prompt-based ransomware variants like "PromptLock 2.0" feature enhanced lateral movement and chaining exploits for maximum impact on target environments.

Cloud Misconfigurations and Identity Compromise in SaaS Ecosystems

November witnessed increased exploitation of cloud misconfigurations and identity theft via OAuth tokens, particularly in collaboration platforms and marketing automation tools. Companies are urged to tighten cloud IAM policies and monitor SaaS integrations for anomalous access.

Deepfake-Facilitated Social Engineering and Synthetic Identity Manipulation

Financial institutions remain prime targets alongside emerging campaigns against power grids and water supply systems. India has issued updated cybersecurity advisories for critical infrastructure in anticipation of increased threat activity during the winter months.

Mobile Identity and 5G Network Exploits

With 5G adoption accelerating, vulnerabilities in SIM swapping, mobile authentication frameworks, and network slice isolation are increasingly exploited for financial and espionage purposes. Regulatory bodies are advancing guidelines to secure next-gen mobile environments.

CYBER NEWS

India's Cybersecurity Ecosystem Scales New Heights

India's cybersecurity industry reached a $20 billion valuation, powered by over 400 startups and a workforce of 650,000 professionals. Advanced threat detection, cyber forensics, and AI-based monitoring systems are increasingly developed, supporting India's drive for a more resilient digital ecosystem. CERT-In leverages AI-driven analytics and automation for real-time detection and incident response, launching coordinated interventions to mitigate the impact of ransomware and other threats.

READ MORE >

Focus on AI's Double-Edged Role

During an EU-Journalist interaction, CERT-In's Director General emphasized that AI acts both as an enabler for defenders—through real-time analytics and automation—and for adversaries, via AI-enabled attacks. India reported 147 ransomware incidents in 2024, but coordinated response and intelligence sharing have helped contain the scale and impact of these events.

READ MORE >

Cloudflare Blames this Week's Massive Outage on Database Issues

The company's Global Network is a distributed infrastructure of servers and data centers across more than 120 countries, providing content delivery, security, and performance optimization services and connecting Cloudflare to over 13,000 networks, including every major ISP, cloud provider, and enterprise worldwide. Matthew Prince, the company's CEO, said in a post-mortem published after the outage was mitigated that the service disruptions were not caused by a cyberattack.

READ MORE >

Surge in SIM Swap and UPI Fraud

In a SIM Swap Scam, cybercriminals trick your mobile operator into issuing a duplicate SIM card of your number. They often claim that the "original SIM is lost or damaged." Once the new SIM is activated, the fraudsters gain control over all your calls, messages, and most critically — your OTPs and banking alerts. Using stolen personal details, they can reset passwords, approve online transactions, and drain funds from your accounts in minutes.

READ MORE >

Critical Vulnerabilities in Windows, CERT-In Warns Users

CERT-In has issued a high-severity alert, warning Windows users in India of several vulnerabilities in Microsoft products and urging them to update their systems immediately. The vulnerabilities, dubbed CIVN-2024-0316, are present in Microsoft Edge (Chromium-based), and arise from inadequate data validation in Mojo, improper implementation in V8, and Integer overflow in Layout.

READ MORE >

CYBER NEWS

White Lock Ransomware Hits Enterprises Worldwide

White Lock ransomware is a newly identified strain targeting Windows environments that combines file encryption with data exfiltration for double extortion. Victims receive ransom notes demanding 4 Bitcoin within four days, with threats to notify customers, sell data to competitors, and publish leaks if unpaid. The malware's adaptable lateral movement and operational sophistication make it a significant threat for large enterprises globally, highlighting the growing trend of strategic and scalable ransomware attacks.

READ MORE >

Jaguar Land Rover UK Ransomware Incident

Jaguar Land Rover suffered the UK's most economically damaging ransomware attack in October 2025, causing $2.5 billion in losses and halting operations for weeks. The attack disrupted manufacturing and the supply chain, impacting over 5,000 partner organizations. This event revealed vulnerabilities in complex industrial networks & the far-reaching effects of ransomware on global supply chains, emphasizing the need for heightened security in critical infrastructure sectors.

READ MORE >

Asahi Breweries Production Shutdown

Japan's leading brewery, Asahi, temporarily ceased production after a highly sophisticated, AI-driven ransomware attack compromised its factory systems. The incident illustrates the increasing use of artificial intelligence by cybercriminals to launch precise and stealthy attacks on manufacturing plants, increasing operational risks and the urgency for improved cybersecurity measures in industrial sectors worldwide.

READ MORE >

KillSec Ransomware Targeting Southeast Asia

WalletKu, an Indonesian digital wallet provider, was targeted by the KillSec ransomware group through a ransomware-as-a-service (RaaS) model, resulting in encrypted systems and leaked customer data on underground forums. This breach underscores the vulnerabilities of fintech platforms in Southeast Asia, fueled by rapid digital adoption and the proliferation of RaaS operations in the cybercrime ecosystem.

READ MORE >

Gentlemen Ransomware Data Leak in Thailand

Thai Future Incorporation, a manufacturer in packaging and film, suffered a ransomware attack by the Gentlemen gang, which leaked extensive internal data including financials, HR, and supply chain information on dark web sites to pressure ransom payment. This attack highlights the expanding ransomware focus on manufacturing and logistics sectors, with significant operational and intellectual property risks.

READ MORE >

01
CASE STUDY

Brief Summary:

A global technology company fell victim to a Business Email Compromise attack that resulted in unauthorized wire transfers totalling $1 million. Attackers gained access to the finance director's corporate email through phishing and social engineering, enabling them to send fraudulent payment instructions to vendors. The breach went unnoticed for over two weeks, leading to significant financial loss and reputational damage.

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

An e-commerce firm experienced a severe security incident when attackers obtained a large set of employee credentials through a third-party password reuse breach. Unauthorized access to internal order management systems allowed attackers to manipulate orders, refund processes, and customer accounts. The breach lasted nearly a month before detection, impacting customer data integrity and causing financial loss due to fraudulent refunds.

Root Cause Analysis:

Credential Reuse and Data Leakage:
Employee credentials were compromised on an unrelated external platform and reused on corporate systems.

Weak Password Policies:
The organization lacked enforced password complexity and rotation policies.

Insufficient Monitoring:
Anomalous login activities were not adequately flagged or investigated in a timely manner.

Loss and Insurance Applicability:

- Losses incurred include fraudulent refunds, customer trust erosion, and heightened customer support costs.
- Regulatory scrutiny and potential fines for lapses in customer data protection.
- Cyber insurance helped cover forensic analysis and notification costs but excluded losses from fraud caused by credential theft.

Recommended Post-Incident Measures:

Enforce strong password policies with mandatory regular changes and complexity requirements.

Integrate Single Sign-On (SSO) with adaptive multi-factor authentication for employee access.

Implement real-time login anomaly detection and immediate incident response triggers.

Conduct workforce training emphasizing risks of password reuse and phishing threats.

DATA SPOTLIGHT

AI-Driven Cyber Threats and Evolving Supply Chain Risks

Supporting Statistics:

- Autonomous AI malware families have increased by 37% in October, exhibiting advanced evasion tactics such as polymorphic code and delayed execution to bypass traditional defenses (Source: Cybervizer, Oct 2025).
- AI-powered phishing campaigns grew by 45%, deploying hyper-personalized deepfake audio and video lures to manipulate victims with unprecedented realism (Source: Cybervizer, Oct 2025).
- Autonomous AI agents scanning and exploiting network vulnerabilities surged by 28%, frequently combining zero-day exploits with automated lateral movement workflows (Source: Cybervizer, Oct 2025).
- Supply chain risks extended further into semiconductor firmware, with several high-profile exploitations reported involving compromised firmware updates disrupting production environments (Source: Cybervizer, Oct 2025).
- Investment in AI-enhanced cybersecurity technologies remains strong, with 87% of IT leaders committing increased budgets toward AI-enabled threat detection and response within the next 18 months (Source: Lakera AI Security Report, Oct 2025).
- Despite rising investments, organizational confidence in AI security readiness remains low at 7%, highlighting urgent needs for integrated governance, continuous training, and threat modeling tailored for AI-driven environments (Source: Lakera AI Security Report, Oct 2025).

Implications and Tactical Risks:

- AI continues to empower advanced persistent threats with autonomous decision-making, requiring defenders to adopt AI-augmented detection and automated response systems.
- Hardware and firmware supply chain vulnerabilities pose critical risks to operational technology and industrial systems, necessitating end-to-end provenance monitoring and secure update mechanisms.
- Cross-disciplinary collaboration between AI specialists, cybersecurity experts, and supply chain stakeholders is essential to develop resilient defense strategies against increasingly complex AI-powered cyber threats.

DPDP RULES ARE HERE – IS YOUR BUSINESS READY?

The DPDP Rules, 2025 Are Now Enforced

India has officially notified the Digital Personal Data Protection (DPDP) Rules, 2025. These rules operationalize the DPDP Act, 2023 and mark the beginning of real privacy enforcement in India. Businesses now face an 18 month transition period to overhaul how they collect, process, secure, and delete personal data.

Compliance Checklist for Businesses

- **Map your data flows –** Identify what personal data you collect, where it is stored, and how it is processed.
- **Update consent mechanisms –** Ensure notices are clear, accessible, and compliant with DPDP standards.
- **Strengthen security controls –** Implement encryption, access restrictions, and breach response protocols.
- **Review vendor contracts –** Align third party processors with DPDP obligations.
- **Train employees –** Build awareness across teams to reduce human error and insider risks.
- **Document compliance –** Maintain records to demonstrate accountability during audits or investigations.

Why This Matters for Your Business?

Accountability is mandatory: Companies must demonstrate lawful data processing and obtain clear consent from individuals.

Data Protection Board of India (DPBI) is now active, empowered to investigate complaints and impose penalties.

Strict obligations: Security safeguards, parental consent for children's data, and regulated cross border transfers are now binding.

Penalties loom large: Non compliance can attract significant fines, reputational damage, and regulatory scrutiny.

Compliance is not optional. Protection is not negotiable. Together, they safeguard your future.

At Edme Insurance Brokers Limited, we are committed to guiding you through this transition. Our cyber insurance solutions are designed to complement your compliance journey, ensuring that your business is not only DPDP ready but also financially protected against evolving cyber risks.

VULNERABILITY WATCH

Microsoft Patch Tuesday October 2025

Microsoft released patches addressing a total of 81 vulnerabilities in its October 2025 Patch Tuesday update. Among these, 10 were rated Critical, including several Remote Code Execution (RCE) flaws affecting Windows Kernel, Hyper-V, and Microsoft Office components. One publicly disclosed zero-day vulnerability was patched in the Windows TCP/IP stack that could allow remote code execution via specially crafted network packets. Several Elevation of Privilege and Information Disclosure vulnerabilities were also fixed. Organizations are urged to prioritize patching due to the presence of actively exploited flaws and high-severity issues in widely deployed enterprise environments.

Adobe Patches for October 2025

Adobe fixed 19 vulnerabilities across Adobe Acrobat, Photoshop, Illustrator, and Adobe Experience Manager. Of these, 11 were critical, including remote code execution and bypass of security features. Immediate updates are recommended to mitigate active exploitation risks especially for enterprises relying on Adobe's creative and document management software.

Google Chrome Security Updates October 2025

Google released security updates addressing 5 vulnerabilities, including a critical zero-day in the V8 JavaScript engine that allows remote code execution via crafted web content. Users are advised to update to Chrome version 141.0.7440.100 or later on all platforms to protect against active exploit campaigns.

SECURITY ADVISORIES

Key Recommendations to Protect Your Business

AI-Driven Cybersecurity Threats and Defenses

AI-driven cybersecurity threats have significantly increased the sophistication and scale of attacks, with cybercriminals leveraging AI to automate vulnerability discovery, craft hyper-personalized phishing campaigns, and deploy adaptive malware that evades traditional defenses. However, AI also empowers defenders by enhancing real-time threat detection, automated response, and predictive analytics, making AI a critical dual-use technology that reshapes cybersecurity strategies worldwide

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

The widespread adoption of Zero Trust security architectures is redefining enterprise defense by eliminating implicit trust and enforcing continuous verification of users, devices, and context before granting access. Zero Trust integrates identity management, endpoint security, and network segmentation to effectively contain breaches and restrict lateral movement, helping organizations strengthen resilience amid increasingly hybrid and cloud-based environments.

CYBER QUIZ

FIND ANSWERS IN
THE NEXT EDITION

What is the primary purpose of a firewall in network security?

A) To encrypt data on the network
B) To monitor employee activity
C) To control incoming and outgoing network traffic based on security rules
D) To create backup copies of data

Which of the following is a common sign of a phishing attack?

A) Receiving unexpected emails with urgent requests for personal information
B) Slow internet connection
C) Pop-up ads on legitimate websites
D) System crashes during startup

ANSWERS FOR OCTOBER CYBER PLUGGED-IN NEWSLETTER QUIZ

Ans: **A** Using polymorphic malware that continuously changes its code to avoid signature-based detection.

Ans: **B** Continuously verify and enforce least-privilege access based on user identity, device health, and context.

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**