# CYBER INSIGHTS DIGEST

September Edition

## NEWS BYTES - DOMESTIC

### SEBI Clarifies Applicability of Cybersecurity Framework

SEBI has issued clarifications on its cybersecurity and cyber resilience framework. The guidelines emphasize critical systems like core operations, client-facing applications, and regulatory data handling, promoting zero-trust principles and robust disaster recovery measures with a 2-hour recovery time objective and 15-minute recovery point objective.

### India Enhances Cybersecurity in Justice System with Digital Tools

Ministry of Home Affairs announced new initiatives, allocating over ₹132 crore for Cyber Forensic-cum-Training Laboratories to support investigations and train personnel in digital forensics. Tools such as e-Sakshya for digital evidence preservation, e-Summon for electronic court summons, and Nyaya-Shruti for video conferencing are improving efficiency and security.

### CyberSecure Andhra 2025 Conference Focuses on Digital Trust

The Confederation of Indian Industry (CII) Andhra Pradesh hosted the 'CyberSecure Andhra 2025' conference on August 21 in Visakhapatnam. The event brought together industry experts, to discuss strategies for effective cyber risk management. Sessions highlighted collaborative approaches to strengthen cybersecurity across sectors in the region

### IndiaTech and APCO Roundtable Bolsters Critical Infrastructure Security

IndiaTech and APCO hosted a closed-door roundtable to secure India's critical information infrastructure in sectors like power, telecom, banking, healthcare, and defense. Discussions focused on protecting digital supply chains, enhancing regulatory frameworks, and promoting public-private collaboration for national cyber resilience.

### CERT-In Introduces Mandatory Annual Cybersecurity Audits

The Indian Computer Emergency Response Team (CERT-In) has mandated annual cybersecurity audits for all companies operating in the digital domain to enhance data protection and compliance. These third-party audits will conduct risk-based assessments on network architecture, application security, cloud infrastructure, and data safeguards, with more frequent reviews for high-risk sectors.

### Mitigata Raises $5.9 Million in Series A for Cyber Resilience Platform

Bengaluru-based cyber resilience startup Mitigata has secured $5.9 million (approximately INR 51.6 crore) in a Series A funding round. The funds will accelerate the development of its AI-driven platform, which provides comprehensive cyber risk assessments, predictive analytics, and integrated cyber insurance solutions tailored for Indian enterprises.

# NEWS BYTES - INTERNATIONAL


## Accenture Acquires CyberCX to Bolster Asia Pacific Defenses Against AI Threats

Accenture announced the acquisition of CyberCX. The deal focuses on countering rising AI-powered threats, including deepfake phishing and automated attacks, through advanced threat intelligence, managed security services, and cloud protections. Partnerships with Microsoft and CrowdStrike will enable proactive defenses, helping organizations transform cybersecurity into a strategic advantage.

## EU Mandates Cybersecurity for IoT Devices Under Updated RED Framework

EU's Radio Equipment Directive (RED) enforces mandatory cybersecurity requirements for all radio-enabled devices, including IoT gadgets, to prevent exploits like Mirai-style botnets. Manufacturers must incorporate secure boot processes, firmware updates, and vulnerability disclosure mechanisms, aiming to safeguard connected ecosystems from remote hijacking.

## UK Bans Ransom Payments to Curb Ransomware Surge in Public Sector

The UK government unveiled plans on August 7, 2025, to ban ransom payments by public entities like the NHS following a spike in ransomware incidents targeting healthcare and local services. This policy shift aims to disrupt cybercriminals' revenue streams, encourage investment in backup and recovery systems, and foster international collaboration.


## Qualys Secures FedRAMP High for Platform Defending Against Nation-State Espionage

Qualys obtained FedRAMP High Authorization for its cloud platform, sponsored by the U.S. DEA, to fortify federal defenses against APTs from nation-state actors. The certification supports vulnerability management, threat hunting, and compliance monitoring, equipping government agencies with tools to detect and respond to espionage campaigns targeting sensitive data in defense and intelligence sectors.

## Qwiet AI Introduces AutoFix Tool to Automate AppSec Against Supply Chain Vulnerabilities

Qwiet AI's AutoFix feature uses generative AI to automatically remediate vulnerabilities in application code, with new integrations for Azure DevOps and GitHub. Designed to address rising supply chain attacks exploiting open-source dependencies, the tool accelerates secure development cycles for DevSecOps teams, enabling faster deployment of resilient software while reducing manual patching.

## Global Cyber Summer School Focuses on Collaborative Defenses Against Hybrid Warfare

The International Cyber Security Summer School trained emerging leaders on countering hybrid cyber-physical threats, such as those blending digital intrusions with kinetic actions in geopolitical conflicts. The program emphasized international policy coordination, AI ethics in defense, and tabletop exercises to build resilient strategies for nations facing coordinated adversary campaigns.

# KEY TRENDS

## 531

**Check Point**

Ransomware attacks publicly reported worldwide in August.

## 3500

**CVE Details**

3500 CVEs (Common Vulnerabilities and Exposures) created in August.

## 1265%

**SentinelOne**

Phishing attacks increased by 1,265% year-over-year, fueled by generative AI tools.

## 275M

**FireCompass**

Patient records compromised in major healthcare sector breaches

## 17.3M

**IT Governance**

Records exposed in global data breaches and cyber attacks.

## 30%

**Verizon**

30% of breaches were linked to third-party involvement

# CYBER INCIDENT ANALYSIS

## Social Engineering Leads to Ransomware Outbreak in Hospitality & Gaming Sector

### INDUSTRY

- Hospitality / Gaming & Entertainment

### BRIEF SUMMARY

- A major hospitality and gaming corporation suffered a catastrophic cyberattack initiated by a social engineering campaign. Threat actors, identified as the 'Scattered Spider' group in affiliation with 'ALPHV/BlackCat' ransomware, used a vishing (voice phishing) attack to gain initial access to the IT helpdesk. This led to widespread ransomware deployment, encrypting critical

### ROOT CAUSE ANALYSIS

- Social engineering (vishing) bypassed helpdesk identity verification for MFA reset.
- Compromised credentials gave attackers access to the core identity platform (Okta)
- Insufficient network segmentation allowed for rapid lateral movement of ransomware.

### LOSS CATEGORIES TO VICTIM

- Operational Disruption, Financial Loss, Data Exposure, Reputational Damage, Regulatory Risk.

### INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Deployed incident response (IR) team for forensic investigation and containment.
- Engaged specialized legal counsel for regulatory and compliance obligations.
- Provided crisis communication experts for managing public relations.

### LOSS INCURRED

- Business Interruption, Remediation Costs, Customer Compensation, Potential Regulatory Fines.

### RECOMMENDED PREVENTIVE MEASURES

- Strengthen helpdesk identity verification protocols for sensitive requests.
- Mandate phishing-resistant MFA (FIDO2) for all privileged accounts.
- Conduct targeted training on vishing tactics for IT support staff.
- Implement Zero Trust architecture to contain lateral movement.

# CYBER INCIDENT ANALYSIS

## Business Email Compromise in a Bank

### INDUSTRY

- Financial Services / Banking

### BRIEF SUMMARY

- A major bank faced a Business Email Compromise (BEC) attack via the "FinSpoof" campaign, using AI-generated deepfake emails and spoofed CFO domains. This enabled ₹15 crore in unauthorized wire transfers by bypassing MFA through session hijacking and vendor invoice manipulation, exploiting urgency in quarterly payments, leading to mailbox and client data

### ROOT CAUSE ANALYSIS

- Phishing emails posing as executive directives tricked finance staff into spoofed portals.
- Adversary-in-the-middle (AitM) proxies captured MFA tokens and sessions.
- Weak DMARC and no anomaly detection allowed token reuse from external IPs.

### LOSS CATEGORIES TO VICTIM

- Financial Losses, Data Exposure, Reputational Damage, Compliance Risk, Operational Disruption

### INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Forensics traced attacker timelines and entry via a vendor portal.
- Threat intel linked FinSpoof to APAC financial campaigns.
- Legal experts handled RBI compliance and law enforcement coordination.

### LOSS INCURRED

- Forensic Analysis, Fraudulent Transfers, Vendor Reimbursements, Regulatory Fines, Phishing-resistant MFA

### RECOMMENDED PREVENTIVE MEASURES

- Use AI email filtering for spoofing detection.
- Enforce full DMARC and audit attachments.
- Run phishing training for finance teams.
- Add approval workflows with payment holds.

# ADVISORIES

## ADVISORY : MICROSOFT PATCHES PUBLICLY DISCLOSED WINDOWS KERBEROS FLAW (CVE-2025-53779)

- **Publicly Disclosed Vulnerability:** As part of its August 2025 Patch Tuesday, Microsoft addressed CVE-2025-53779, a publicly disclosed elevation of privilege vulnerability in Windows Kerberos. The flaw was known before a patch was available.
- **Potential for Domain Compromise:** A successful exploit could allow an authenticated attacker to gain full domain administrator privileges, leading to a complete compromise of an Active Directory environment.
- **Recommended Action Update:** Administrators are strongly urged to apply the August 2025 security updates to all Windows Servers immediately. This vulnerability is rated as high priority due to its public disclosure.
- **Affects Modern Servers:** The vulnerability specifically impacts environments with at least one domain controller running Windows Server 2025, making it critical for organizations adopting the latest OS to patch.

**Read more at: Microsoft Security Response Center - CVE-2025-53779**

## ADVISORY : IVANTI RELEASES PATCHES FOR MULTIPLE CRITICAL PRODUCT VULNERABILITIES

- **Multiple Products Affected:** Ivanti published security advisories addressing multiple new vulnerabilities in its product suite, including Ivanti Connect Secure (ICS), Policy Secure, and ZTA Gateways.
- **Focus on Denial of Service:** The advisory details several high-severity flaws that could be exploited by a remote, unauthenticated attacker to trigger a denial of service (DoS), causing a complete outage of the targeted appliance.
- **Mitigation Recommendations Provided:** Ivanti has released patched software versions for all affected products and urges customers to update their environments to the latest builds to protect against these vulnerabilities.
- **Targets Public and Private Sectors:** The guidance is intended for all organizations that rely on Ivanti's secure access solutions to proactively remediate and defend their network perimeter from potential attacks.

**Read more at: Ivanti Community - August 2025 Security Advisory**