GLOBAL NEXT CONSULTING INDIA PRIVATE LIMITED

GNCIPL

(Leader In Consulting)

www.gncipl.com|www.gncipl.online

Cybersecurity Daily News Analysis(C-DNA) Across the Globe

22 May 2025

🔒 Major Data Breaches & Cyberattacks

- **Coca-Cola Suffers Dual Cyberattacks**
  Two hacking groups, Everest and Gehenna, have claimed responsibility for breaching Coca-Cola's systems. The Everest group reportedly exfiltrated sensitive internal data, while Gehenna alleges the theft of over 23 million records from Coca-Cola Europacific Partners' Salesforce database, primarily affecting operations in the Middle East. Cyber Security News

- **Marks & Spencer Faces £300 Million Loss Due to Cyberattack**
  British retailer Marks & Spencer experienced a significant cyberattack, resulting in a projected £300 million loss. The breach disrupted online transactions and store operations, with recovery efforts expected to continue into July. Medium+1Reuters+1

- **Lumma Stealer Malware Network Disrupted**
  A collaborative operation by global law enforcement and private sector partners has dismantled the infrastructure of the Lumma Stealer malware network, which had infected approximately 10 million systems. Authorities seized over 2,300 domains used to control compromised machines. CyberScoop+2The Hacker News+2Cybersecurity Dive+2

🛡️ Government & Industry Cybersecurity Initiatives

- **SEBI Eases Cybersecurity Compliance for Smaller Entities**
  India's Securities and Exchange Board (SEBI) has issued clarifications to simplify

cybersecurity compliance requirements for smaller market participants, aiming to enhance overall cyber resilience in the financial sector. BW Legal World

- **Moldova Moves Closer to Joining EU Cybersecurity Reserve**
  Moldova has taken significant steps toward integrating with the European Union's Cybersecurity Reserve, signaling a commitment to bolstering its national cyber defense capabilities. EU Neighbours East

- **CISA Warns of Russian Cyber Threats to Tech Firms**
  The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued an advisory about Russian military-affiliated cyber actors targeting logistics and technology companies in the U.S. and allied nations, highlighting the need for heightened vigilance. Inside Cybersecurity

---

🧠 AI & Emerging Cybersecurity Trends

- **AI: A Double-Edged Sword in Cybersecurity**
  Artificial intelligence is increasingly being used both to enhance cybersecurity defenses and to execute sophisticated cyberattacks. Experts emphasize the importance of developing robust AI governance frameworks to mitigate associated risks. McKinsey & Company

- **Post-Quantum Cryptography Gains Traction**
  Microsoft is advancing post-quantum cryptographic solutions to prepare for future threats posed by quantum computing, aiming to protect organizational data against potential quantum-enabled breaches. UC Today

---

🏥 Sector-Specific Cybersecurity Developments

- **Education Sector Lags in Data Breach Reporting**
  A recent study reveals that educational institutions take an average of 4.8 months to report data breaches, the longest among all sectors, underscoring the need for improved incident response protocols in education. Higher Ed Dive

- **Kettering Health Cyberattack Disrupts Services**
  Kettering Health in the U.S. experienced a ransomware attack that disrupted patient services and led to the cancellation of elective procedures, highlighting vulnerabilities in healthcare cybersecurity. Industrial Cyber

---

🧰 Notable Vulnerabilities & Exploits

- **BIND DNS Server Vulnerability Exploited**
  Attackers have exploited a vulnerability in BIND DNS server software (CVE-2023-5517), causing servers to crash through specially crafted packets. Administrators are urged to apply patches promptly. GBHackers
- **Cisco and Atlassian Release Security Patches**
  Cisco and Atlassian have issued patches addressing multiple high-severity vulnerabilities in their products, including issues in Cisco's Identity Services Engine and Atlassian's software offerings. SecurityWeek
- 🛡️ **Government Policies & Regulatory Actions**
- **Japan Enacts Active Cyberdefence Law**
  Japan has passed the Active Cyberdefence Law (ACD), empowering authorities to proactively monitor and neutralize foreign cyber threats. This legislation marks a significant shift from previous limitations imposed by Japan's pacifist constitution and strong privacy laws, particularly Article 21, which restricted surveillance and wiretapping. The ACD permits the government to track IP communications between Japan and foreign nations and mandates critical infrastructure operators to report breaches .Financial Times
- **Hong Kong Introduces New Cybersecurity Legislation**
  Hong Kong has enacted a cybersecurity law aimed at securing critical infrastructure across eight industries, including banking, IT, energy, healthcare, and communications. Effective from 2026, the law requires operators to enhance their systems, conduct annual risk assessments, and report serious incidents within two hours. Penalties for non-compliance can reach up to HK$5 million ($640,000) .Reuters
- ---
- 🔒 **Regional Threat Landscape**
- **Surge in Ransomware and Malware Attacks**
  The Asia-Pacific region is experiencing a significant increase in ransomware and malware attacks, particularly targeting critical infrastructure. In the first half of 2024 alone, over 57,000 ransomware incidents were reported, with Indonesia, the Philippines, and Thailand being the most affected. Attackers are employing double and triple extortion tactics, threatening to leak sensitive data or disrupt vital services .Access Partnership

- **Advanced Persistent Threats (APTs) on the Rise**
  State-sponsored cyber espionage campaigns, such as the "MirrorFace" operation believed to be backed by China, are increasingly targeting government and corporate systems in the region. These APTs pose significant risks to national security and economic stability .Financial Times

- ---

- 💼 **Corporate Initiatives & Industry Developments**

- **Datadog Expands Local Data Center Capacity in Australia**
  In response to increasing regulatory scrutiny about offshore data transfers, U.S. cybersecurity firm Datadog has announced plans to establish local data center capacity in Australia. This move aligns with the broader trend of data repatriation and aims to meet stringent data sovereignty requirements. Datadog serves over 1,000 clients in Australia and New Zealand and sees the region as a high-priority market .The Australian

- **SentinelOne Recognizes Asia-Pacific Cybersecurity Partners**
  At the 2025 APJ PartnerOne Summit in Bangkok, SentinelOne honored innovative cybersecurity partners across the Asia-Pacific and Japan region. The awards recognized outstanding contributions to security solutions and highlighted the importance of collaboration in enhancing enterprise security .Business Wire

- ---

- 📊 **Regional Cybersecurity Maturity**

- **India Leads in Cybersecurity Maturity**
  India has achieved the highest cybersecurity maturity score in the Asia-Pacific region, according to a report by Palo Alto Networks and Tech Research Asia. Indian companies allocate an average of 13% of their revenue to cybersecurity, with plans to increase AI and security spending by over 41%. This positions India as a regional benchmark for digital protection .DQ

-