INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

SEBI'S NEW CYBERSECURITY FRAMEWORK

In a significant move to bolster cybersecurity within India's financial sector, the Securities and Exchange Board of India (SEBI) announced the launch of its Cybersecurity and Cyber Resilience Framework (CSCRF) on 20 August 2024. This new framework is set to enhance the cybersecurity measures of SEBI-regulated entities, ensuring that they are well-prepared to tackle the increasingly sophisticated cyber threats facing the industry.

IN THIS NEWSLETTER

The CSCRF is designed to provide a structured approach for protecting critical financial systems and data, focusing on both prevention and response to cyber incidents. It introduces a comprehensive set of guidelines and standards that regulated entities, including Alternative Investment Funds (AIFs), Stock Exchanges, Mutual Funds, and others, must adhere to.

Key Highlights of the CSCRF:

- **Anticipate and Prevent Threats:** The framework emphasizes on the importance of maintaining a state of informed preparedness to foresee and prevent cyber threats.
- **Ensure Continuity:** It outlines measures to ensure that essential business functions continue even in the face of cyber-attacks.
- **Rapid Recovery:** The CSCRF includes detailed guidelines for restoring systems quickly after an incident, minimizing downtime and impact.
- **Continuous Improvement:** The framework encourages entities to continuously evolve and improve their cybersecurity strategies to stay ahead of emerging threats.

SEBI has set clear timelines for the implementation of CSCRF, with entities required to comply with the new standards by 01 January 2025, for those with existing cybersecurity frameworks and by 01 April 2025, for others.

Implications for the Financial Sector

The introduction of the CSCRF is expected to significantly enhance the resilience of India's financial markets. By adhering to the framework, entities regulated by SEBI will not only improve their cybersecurity posture but also contribute to the overall stability of the financial ecosystem.

Industry experts have welcomed the move, highlighting that the CSCRF will play a crucial role in safeguarding investor interests and maintaining trust in the financial system. With cyber threats becoming more sophisticated, the framework is seen as a necessary step to ensure that all regulated entities are adequately protected.

As cyber risks continue to evolve, CSCRF is poised to be a cornerstone in the ongoing efforts to strengthen cybersecurity across the financial sector. Entities are encouraged to begin implementing the framework's guidelines and to take proactive steps towards achieving full compliance.

CRITICAL ANDROID VULNERABILITY AFFECTS PIXEL DEVICES

A critical vulnerability has been identified in an Android package named Showcase.apk, which has been preinstalled on numerous Pixel devices since 2017. This package has extensive system permissions that enable remote code execution and package installation. It retrieves configuration files via unsecured HTTP from a single U.S.-based AWS domain, making it susceptible to tampering. The combination of excessive privileges and insecure configuration exposes millions of Pixel devices to man-in-the-middle attacks, which can lead to malicious code injection and spyware infiltration.

Showcase.apk, bundled within Google's OTA images, is a significant security concern. Malicious actors can exploit weaknesses in the application's infrastructure to execute code or shell commands with system privileges, potentially leading to device takeover and facilitating cybercrime. Despite the application being disabled by default, it can be activated through various methods, including physical access. Currently, a patch or software removal to address this issue has not been released by Google.

This vulnerability also allows unauthorized remote code execution due to the applications privileged system-level status and its inability to be uninstalled. The preinstallation of Showcase.apk highlights critical security risks associated with third-party applications operating at the system level, emphasizing on the need for rigorous security testing and increased transparency in software integration.

AFRICA'S ECONOMY FACES CYBERSECURITY DEFICIT

As Africa experiences rapid economic growth, cybercrime is rising, significantly impacting the continent's development. The average number of weekly cyberattacks on African businesses grew by 23 per cent in 2023 compared to previous years, making Africa the region witnessing the fastest increase in cyber threats, across the globe, according to the Interpol 2024 African Cyberthreat Assessment. Ransomware and business email compromise (BEC) top the list of serious threats.

Challenges such as digital illiteracy, aging infrastructure and a lack of security professionals hinder efforts to prevent economic loss due to cybercrimes, as highlighted in a report by Access Partnership and the Centre for Human Rights at the University of Pretoria, South Africa.

With Africa's GDP expected to reach $4 trillion by 2027, the impact of cyberattacks poses a significant threat to economic development, of the continent. Nicole Isaac, Vice President of Global Public Policy for Cisco, emphasized on the urgency of addressing these challenges, stating that Africa faces the most significant impact from cyber threats compared to any other continent. Financial leaders across Africa consider cybercrime a major threat alongside macroeconomic factors and political instability.

In South Africa, cybercrime costs the economy approximately 2.2 billion Rand (approximately US $123 million) annually, largely due to a general lack of cybersecurity awareness, according to Heinrich Bohlmann, Associate Professor in the Department of Economics at the University of Pretoria. Most of the incidents of cybercrimes result from users unknowingly falling victim to scams, which can have severe consequences for businesses.

The rise in cybercrimes should be viewed as an opportunity, especially as Africa undergoes a digital transformation. Africa is seen as a source of young, tech-savvy workers who will be well-positioned to use new technologies, such as artificial intelligence (AI), to enhance business and cybersecurity.

Caroline Parker, Managing Director, FTI Consulting, South Africa, stressed on the importance of governments developing robust regulatory frameworks to enhance cybersecurity. She highlighted the need for regional collaboration, stating that challenges in cybersecurity cannot be addressed by individual governments alone, given the cross-border nature of cyber threats.

AI is expected to play a crucial role in Africa's future, with the economic value of AI in sub-Saharan Africa projected to contribute more than US $130 billion in growth, according to the "Elevating Africa's Cyber Resilience" report by Access Partnership and the University of Pretoria. AI can empower underrepresented groups by providing them with the skills and opportunities to safely participate in the digital economy.

The report also highlights the need for more accurate data on the cost of cybercrimes in Africa. Current estimates, often lacking supporting evidence, suggest that cybercrimes could cost African economies 10 per cent of their GDP. However, more reliable estimates place the cost at between $4 billion and $10 billion annually, or around 0.3 per cent of Africa's GDP.

VULNERABILITIES AI PLATFORMS EXPOSE SENSITIVE DATA

It is a given that artificial intelligence (AI) platforms, have become essential tools for businesses worldwide. However, recent investigations have revealed critical vulnerabilities in such platforms. These vulnerabilities expose sensitive data to unauthorized access, posing significant risks to data security.

AI platforms, including chatbots powered by large language models (LLMs) and machine learning operations (MLOps), are widely used to automate tasks, manage data and interact with customers. However, a comprehensive study by Legit Security, a cybersecurity firm based in Tel Aviv has uncovered serious security threats, particularly in vector databases and LLM tools.

Publicly Exposed Vector Databases

Vector databases store data as multi-dimensional vectors and are commonly used in AI architectures, such as retrieval-augmented generation (RAG) systems. Popular platforms include Milvus, Qdrant, Chroma, and Weaviate. Despite their utility, many vector databases are publicly accessible without proper authentication, allowing unauthorized users to access sensitive information, including personally identifiable information (PII), medical records and private communications.

The investigation found approximately 30 servers containing sensitive corporate and private data, such as company email conversations, customer PII, product serial numbers, financial records and candidate resumes. In one case, a Weaviate database from an engineering services company contained private emails, while another instance involved a Qdrant database with customer details from an industrial equipment firm.

Publicly Exposed LLM Tools

Low-code platforms like Flowise enable users to build AI workflows by integrating data loaders, caches and databases. However, these tools are vulnerable to data breaches if not properly secured. The study identified a critical vulnerability (CVE-2024-31621) in Flowise, which allows authentication bypass through simple URL manipulation. Exposed Flowise servers were found to return unauthorized access errors on any API request, indicating severe security flaws.

Key Findings

The research revealed numerous exposed secrets, including OpenAI API keys, Pinecone API keys, and GitHub access tokens. These vulnerabilities could lead to significant data breaches if not addressed.

Mitigation Strategies

To mitigate these risks, organizations should enforce strict authentication and authorization protocols, regularly update software to patch known vulnerabilities, conduct thorough security audits and educate staff on best practices for data protection.

SOUTH KOREAN APT USES WPS OFFICE BUG FOR INTEL ON CHINA

Earlier this year, a South Korean advanced persistent threat (APT) group, APT-C-60, exploited a critical vulnerability in WPS Office, a widely used office software in China, to conduct cyber espionage against high-level entities. WPS Office, a free competitor to Microsoft Office, boasts 600 million monthly active users, particularly in China, where it dominates the market with over 90 per cent share in mobile office software. The software is extensively used across government agencies, telecommunications companies and other major sectors, making it an attractive target for hackers.

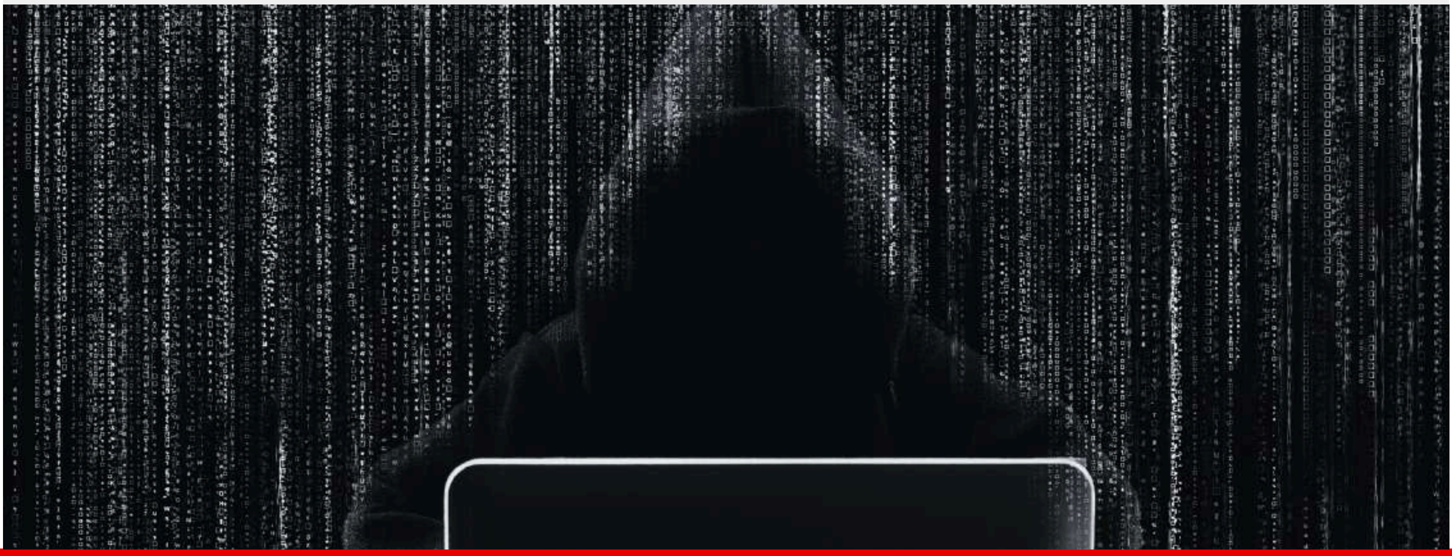
Exploitation by APT-C-60

The South Korea-aligned cyberespionage group, APT-C-60, also known as Pseudo Hunter, is known for targeting entities within South Korea. In this recent campaign, the group delivered a custom backdoor, dubbed "SpyGlace," to WPS users through an arbitrary code execution exploit. The objective of this operation was to gather intelligence on China-South Korea relations.

The vulnerability in WPS Office allowed APT-C-60 to exploit a component known as promecefpluginhost.exe, which did not properly validate file paths used to load plug-ins into the programme. Instead of directly loading malware, APT-C-60 used a custom protocol handler registered by WPS, known as ksoqing://, to execute external applications, tricking the software into loading malicious code.

CVE-2024-7262: The Initial Bug

This vulnerability, tracked as CVE-2024-7262, was given a critical severity rating of 9.3 out of 10 on the CVSS scale. It affected WPS Office for Windows from version 12.2.0.13110, released about a year ago, until the patch in March, with version 12.1.0.16412. The exploit allowed attackers to deliver the SpyGlace backdoor by embedding malicious code in an MHTML file, a web archive file format that encapsulates the contents of a webpage into a single file. When victims clicked on what appeared to be a normal spreadsheet cell, they unknowingly triggered the download of the malicious backdoor.



CVE-2024-7263: The Second Vulnerability

In March, Kingsoft, the developer of WPS Office, implemented a twofold fix for CVE-2024-7262. However, the fix missed another parameter that allowed the same type of vulnerability. This oversight led to the discovery of the second critical vulnerability, tracked as CVE-2024-7263, which also received a 9.3 severity rating, on the CVSS scale. Although the second vulnerability was likely patched by late spring, the situation underscores the importance of promptly addressing security flaws.

Call to Action

With both critical bugs now accounted for, experts urge all WPS Office users to patch their software immediately. The exploitation of these vulnerabilities serves as a stark reminder of the risks posed by unpatched software. As APT groups continue to exploit such weaknesses, it is crucial for users to keep their systems updated and exercise caution when interacting with potentially malicious files.

U.S. OFFERS $2.5 MILLION FOR ANGLER EXPLOIT KIT DEVELOPER

The U.S. Department of State has announced a reward of up to $2.5 million for information leading to the arrest and/or conviction of Volodymyr Kadariya, the key figure allegedly involved in developing and distributing the Angler Exploit Kit (AEK). This sophisticated tool has been used by cybercriminals to deliver malware to unsuspecting users worldwide.

Charges Against Volodymyr Kadariya

Kadariya has been indicted in the District of New Jersey on multiple charges, including conspiracy to commit wire fraud, conspiracy to commit computer fraud and two counts of substantive wire fraud. These charges stem from his alleged involvement in a scheme to distribute the Angler Exploit Kit and other malware through online advertisements, known as "malvertising," from October 2013 to March 2022. The Angler Exploit Kit has been a leading vehicle for cybercriminals, affecting millions of Internet users globally.

The Angler Exploit Kit: A Cybercriminal's Tool

The Angler Exploit Kit is recognized as one of the most sophisticated exploit kits in the world. It first appeared in late 2013 and has since evolved, incorporating advanced evasion features to bypass security defenses. The kit employs techniques such as 302 cushioning and domain shadowing to evade detection and checks for antivirus software and virtualized environments before executing exploits. One of its notable features is "fileless infection," allowing it to infect a victim's system without writing malware to the hard drive.

The Angler Exploit Kit has exploited zero-day vulnerabilities, including those associated with the infamous "Hacking Team" vulnerabilities (CVE-2015-5119, CVE-2015-5122). Its ability to continually add new IP addresses, domains and subdomains for hosting exploits makes it a formidable challenge for cybersecurity professionals.

How does the Angler Exploit Kit Operate?

The Angler Exploit Kit begins its attack by compromising legitimate websites, redirecting visitors to its landing pages through various methods, including HTML iframes and 302 cushioning. These landing pages are highly obfuscated, using techniques such as plain English text, obfuscated JavaScript code, encrypted URLs and exploit paths. This complexity makes it difficult for security researchers to detect and analyze the kit's activities.

The kit also performs environment checks, looking for specific antivirus products and virtual machine indicators to avoid detection. Once these checks are passed, the kit proceeds to decrypt URLs and download the malware payload, often encrypted and encoded to evade detection further.

Global Efforts to Capture Kadariya

The U.S. Department of State's reward offer underscores the international effort to combat cybercrimes. Individuals with information about Kadariya's whereabouts are urged to contact the U.S. Secret Service at MostWanted@usss.dhs.gov. Those located outside the United States can contact the nearest U.S. Embassy or Consulate.

The impact of the Angler Exploit Kit on global cybersecurity cannot be overstated. Its ability to adapt and evade detection has made it a preferred tool for cybercriminals, contributing to the proliferation of malware attacks worldwide. The arrest and conviction of Volodymyr Kadariya would be a significant victory in the fight against cybercrimes.

The $2.5 million reward reflects the seriousness with which the U.S. Government views this threat. As cybersecurity threats continue to evolve, international cooperation and vigilance remain crucial in protecting individuals and organizations from cybercriminal activities.

```
import "../index.css";
import { ReactComponent as ArrowIcon } from "../assets/icons/arrow.svg";
import { ReactComponent as BoltIcon } from "../assets/icons/bolt.svg";
import { ReactComponent as RightArrowIcon } from "../assets/icons/right-arrow.svg";

import React, { useState, useEffect, useRef } from "react";
import { CSSTransition } from "react-transition-group";
```

```
import React, { useEffect } from "react";
import { CSSTransition } from "react-transition-group";
import "../../index.css";
import "./modal.css";

const Modal = (props) => {
 //set close by state

 //set close by "esc"
 const closeOnEscapeKeyDown = (e) => {
  if (e.charCode || e.keyCode === 27) {
   props.onClose();
  }
 };

 //use effect to detect click "esc"
 useEffect(() => {
  document.body.addEventListener("keydown", closeOnEscapeKeyDown);
  return function cleanup() {
   document.body.removeEventListener("keydown", closeOnEscapeKeyDown);
  };
 }, []);
```

DOT RELEASES DRAFT RULES FOR CONSULTATION

The Department of Telecommunications (DoT), Government of India has released four sets of draft rules under the Telecommunications Act, 2023, for a 30-day consultation period on 30 August 2024. These rules cover areas like interception, suspension of telecom services, telecom cybersecurity and critical telecom infrastructure.

Interception Rules

The draft rules maintain the authority of the union or state home secretaries to issue interception orders, like the existing Rule 419A of the Telegraph Rules, 1951. In exceptional circumstances, an authorized joint secretary-level officer or an inspector general of police in remote areas may issue such orders. The interception orders are limited to five reasons, including national security and public order and can remain in force for up to 60 days, with a maximum extension of 180 days.

Concerns have been raised regarding the provision for the destruction of interception orders, as it may lead to a lack of accountability. The draft rules introduce four key changes, including the requirement for DoT to authorize nodal officers to handle interception orders and the inclusion of telecom entities beyond telcos. Additionally, the draft rules remove provisions for fines or license suspensions for unauthorized interceptions, making telecom entities responsible for the actionsn of their employees' and vendors.'

Telecom Suspension Rules

The draft rules for suspending telecom services remain largely unchanged, with new provisions requiring the publication of suspension orders and limiting their duration to 15 days. The review committee structure remains the same, but the rules permit the committee to set aside orders that do not meet prescribed standards. Critics argue that the process remains executive-led, with no judicial or parliamentary oversight, potentially leading to unconstitutional practices.

Telecom Cybersecurity Rules

The draft telecom cybersecurity rules mandate telecom entities to implement measures to prevent and respond to cyber incidents. The central government or authorized agencies can request traffic data from telecom entities for cybersecurity reasons. The rules require the appointment of a chief telecommunication security officer, the adoption of a cybersecurity policy and periodic audits. The rules also prohibit tampering with International Mobile Equipment Identity (IMEI) number and mandate registration of IMEI numbers for both domestically manufactured and imported equipment.

Critical Telecom Infrastructure Rules

Under the proposed Critical Telecommunication Infrastructure (CTI) Rules, the government can notify certain telecom networks as critical infrastructure if their disruption would have a significant impact on national security or public safety. Authorized personnel may inspect hardware, software, and data related to CTI, and the chief telecommunication security officer will be responsible for implementing these rules.

These draft rules are now open for public consultation, and stakeholders are encouraged to provide their feedback within the 30-day period.

MALWARE ATTACKS IN INDIA UP 11%, RANSOMWARE UP 22%

Malware attacks in India have risen by 11 per cent in 2024, reaching a total of 13,44,566 incidents compared to 12,13,528 in 2023, according to the 2024 SonicWall Mid-Year Cyber Threat Report. SonicWall is a California based cybersecurity firm. The report also highlights a significant 22 per cent increase in ransomware attacks during the same period.

Key Findings:

- **Malware Attacks:** The total number of malware attacks saw an 11 per cent increase, reflecting the growing threat landscape.
- **Surge in Ransomware attacks:** Incidents of ransomware attacks went up by 22 per cent, emphasizing the escalating risk to organizations.
- **IoT Attacks:** Attacks targeting Internet of Things (IoT) devices surged by 59 per cent, reaching 16,80,787 incidents in 2024 from 10,57,320 incidents in 2023.
- **Crypto Attacks:** There was a staggering 409 per cent increase in crypto attacks, during the same period, highlighting a new area of concern.

The report indicates that organizations faced a potential of 46 days of downtime due to cyber attacks, with businesses experiencing an average of 1,104 hours of critical attacks during 880 working hours.

SonicWall Vice President, APJ Sales, Debasish Mukherjee, noted that organizations are dealing with an increasingly dynamic threat landscape, where attackers are continually innovating to evade defences. The report also revealed that 78,923 new malware variants were identified in the first five months of 2024, with over 500 new strains discovered daily.

Globally, the total malware volume increased by 30 per cent in the first half of 2024, with a notable 92 per cent rise in May 2024. Although cryptojacking has decreased by 60 per cent globally, India remains an exception, experiencing a rise in such attacks.

TELEGRAM UNDER SECURITY REVIEW

Telegram, a popular messaging application, is currently under intense scrutiny in India due to its involvement in various criminal activities. These include distribution of leaked exam papers, child pornography, stock price manipulation and extortion, drawing parallels to the dark web, according to cyber experts, law enforcement officers, and former government officials.

Recent Developments

- **Global Attention**
  - Telegram CEO Pavel Durov was detained in France on 24 August 2024, over allegations related to implementation of inadequate measures against proliferation of crime on the platform, including the spread of child sexual abuse material. This incident has heightened global focus on Telegram's challenges in law enforcement and content moderation.

- **Indian Cases**
  - On 24 July 2024, the Securities and Exchange Board of India (SEBI) revealed a stock-price manipulation scheme conducted via Telegram, with a group owner indicted for a ₹20 lakh commission related to a listed steel sheet manufacturing company.
  - On 03 May 2024, two men from Bhopal were arrested for duping a local doctor of ₹38 lakh using Telegram to impersonate police officers in a fake interrogation.
  - The cancellation of the UGC-NET exam on 19 June 2023, happened due to a paper leak on Telegram. Similarly, NEET-UG examination papers were reportedly leaked on Telegram.

Law Enforcement Challenges

- **Criminal Activities**
  - Investment fraud, fake SIM card sales and bank account scams are prevalent on Telegram. The platform's anonymity feature makes it difficult for investigators to trace individuals involved in malicious activities.

- **Cooperation Issues**
  - Telegram's cooperation with Indian law enforcement has been limited. The platform reportedly provides minimal assistance, often offering only the last login's IP address, which is of little use in investigations.

- **Regulatory Compliance**
  - Despite appointing a grievance officer and opening an office in Gurugram, Telegram's compliance with Indian IT Rules 2021 has been inconsistent. The platform has faced criticism for its lack of proactive content moderation and transparency.

Despite Telegram's efforts to moderate content, including banning numerous channels related to child abuse, the platform's challenges in balancing privacy with security continue to attract significant scrutiny and criticism.

CRITICAL INFRASTRUCTURE WITNESSES SPIKE IN CYBERATTACKS

India's critical infrastructure, spanning sectors like finance, government, manufacturing and healthcare is experiencing a significant rise in cyberattacks and threats. The surge in cyber incidents has prompted urgent calls for enhanced cybersecurity measures from institutions like the Reserve Bank India (RBI), the banking regulator.

Recent Developments

- **Increased Cyber Incidents**
  - In April 2024, a hacking group leaked 7.5 million records containing personal information from India's leading wireless audio and wearable devices manufacturer, Boat.
  - According to the RBI, cyber incidents against financial institutions and handled by CERT-In soared to approximately 16 million in 2023, which is an astronomical rise from 53,000 incidents in 2017.

- **Sector-Specific Threats**
  - The financial sector is grappling with cybersecurity challenges as it transitions to digital technologies. The RBI report highlights concerns about digitalization posing risks to financial stability due to cybersecurity threats and data breaches.
  - Public sector and government systems are also seeing a notable rise in cyberattacks. A Trojan named HackBrowserData has targeted government agencies and energy companies.

- **Cybersecurity Rankings**
  - India is ranked fourth in the Asia-Pacific region for cybersecurity incidents, with 83 per cent of organizations reporting at least one incident in the past year. This places India behind countries like Vietnam (94 per cent), New Zealand (90 per cent) and Hong Kong (86m per cent).

Top Cybersecurity Concerns

- **Emerging Threats**
  - Indian organizations are particularly worried about cloud-related threats (52 per cent), attacks on connected devices (45 per cent), hack and leak operations (36 per cent) and software supply chain compromises (35 per cent), according to PwC's, The C-Suite Playbook report.
  - The rise of artificial intelligence (AI) and digital transformation has heightened the need for robust security measures. AI-enabled phishing and aggressive social engineering have made ransomware attacks a top concern.

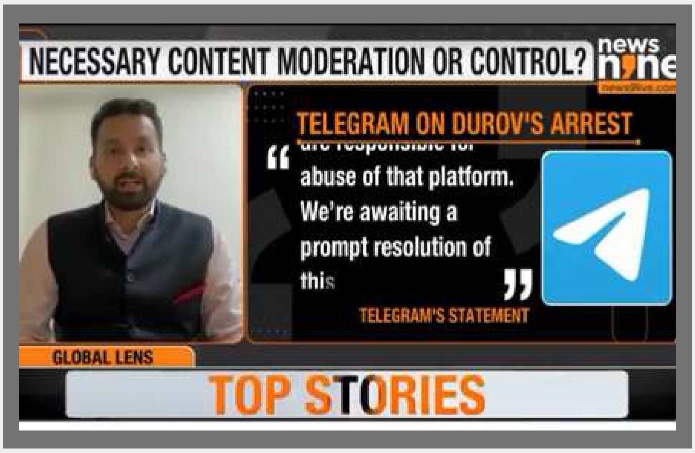
- **Insider Threats**
  - There is an increasing need for organizations to defend against insider threats. This requires improvements in business strategy, culture, training and governance processes.

- **AI in Cybersecurity**
  - The demand for AI is reshaping the threat landscape, with threat actors using AI to create customized and polymorphic malware that can evade traditional detection methods. This makes it crucial to address the AI skills gap within Indian businesses and enhance regular trainings in employing AI in the realm of cybersecurity.

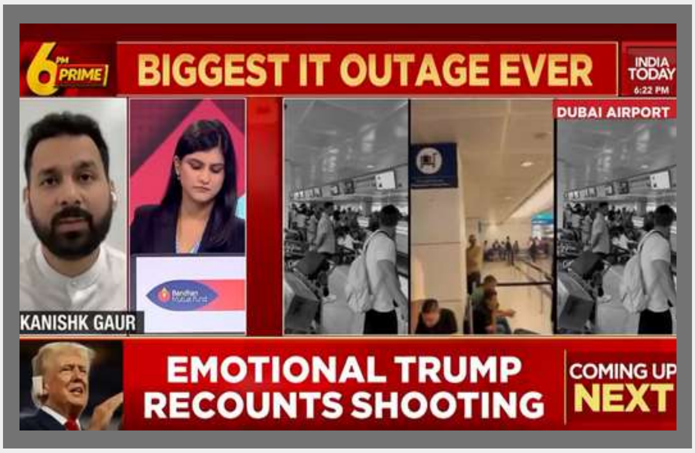
- **Legislative Concerns**
  - Experts are of the view that there is a need for updated legislation. The current Information Technology Act 2000 is seen as outdated to address contemporary cyber threats.

The evolving threat landscape, driven by advancements in AI and increased digital interconnectivity, requires India to bolster its cybersecurity frameworks. Enhancing both technology defences and skills training will be essential in mitigating/countering future cyber threats and ensuring the security of critical infrastructure.

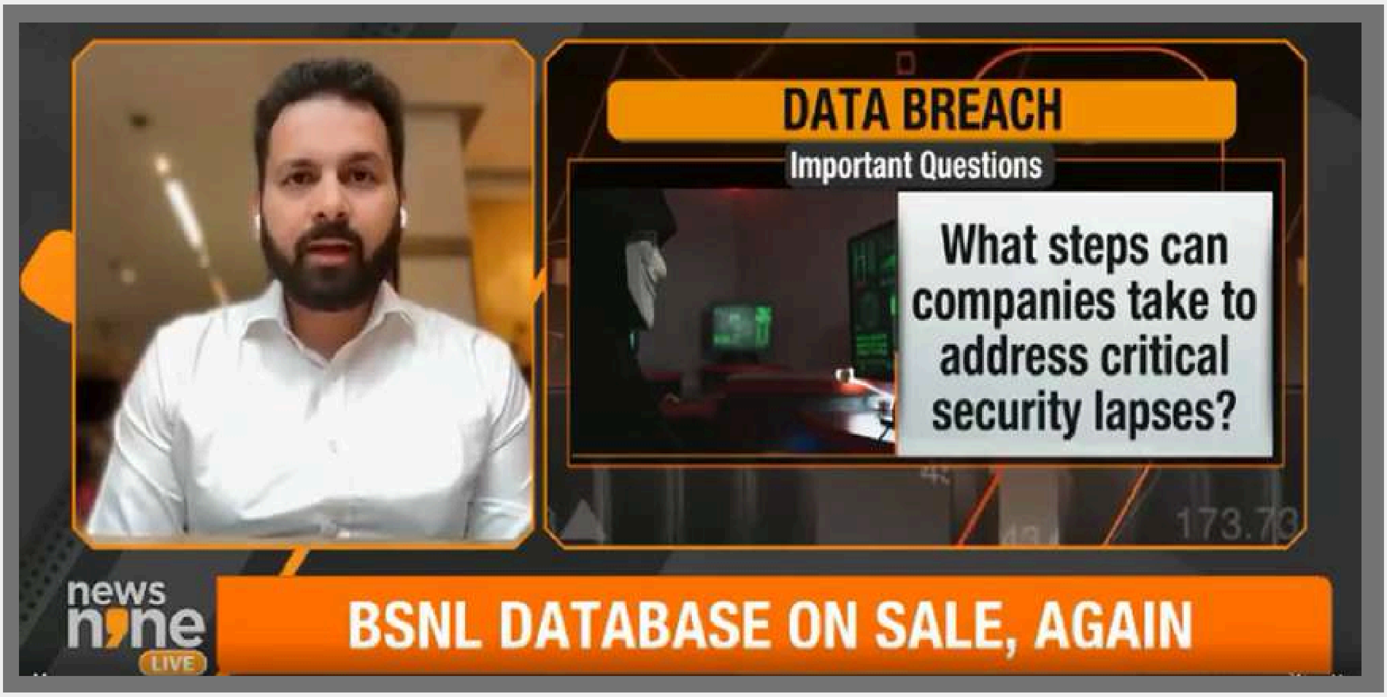
IFF IN THE MEDIA


NECESSARY CONTENT MODERATION OR CONTROL?
news nine
TELEGRAM ON DUROV'S ARREST
"are responsible for abuse of that platform. We're awaiting a prompt resolution of this"
TELEGRAM'S STATEMENT
GLOBAL LENS
TOP STORIES

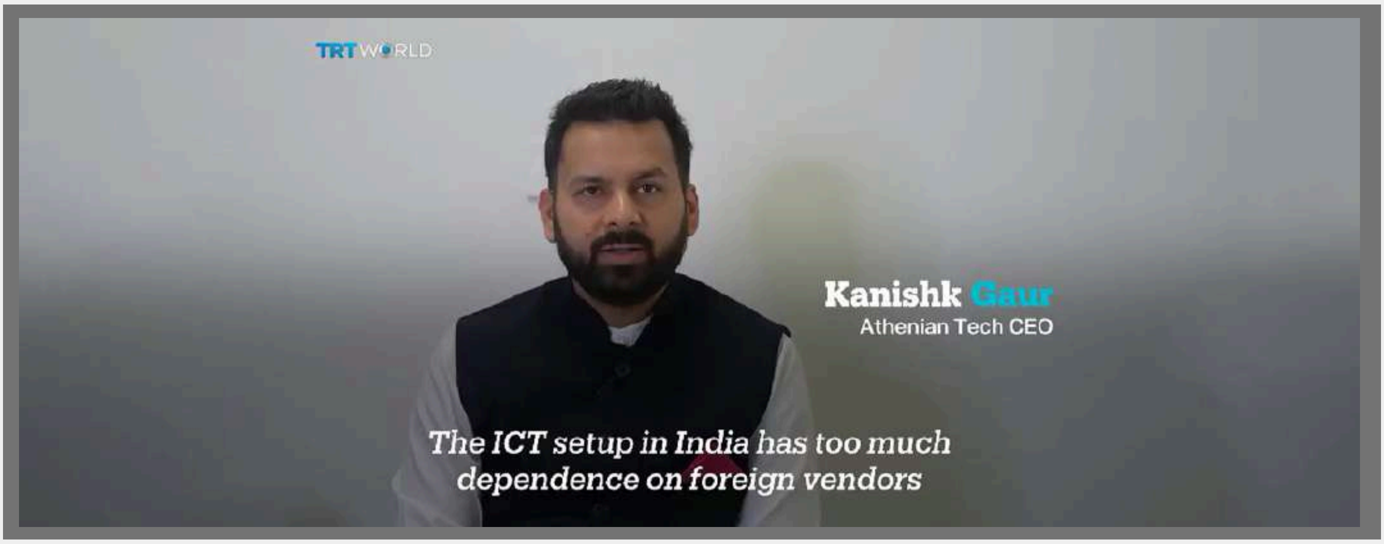
Kanishk Gaur, Founder & CEO, IFF, discussed the scrutiny over Telegram on *newsnine.*



Kanishk Gaur, Founder & CEO, IFF, addressed CrowdStrike's resilience lapse on *India Today.*


DATA BREACH
Important Questions
What steps can companies take to address critical security lapses?
news nine
LIVE
BSNL DATABASE ON SALE, AGAIN

Kanishk Gaur, Founder and CEO of IFF, shared his insights on BSNL's Data Breach with *newsnine.*


TRT WORLD
Kanishk Gaur
Athenian Tech CEO
The ICT setup in India has too much dependence on foreign vendors

Kanishk Gaur, Founder & CEO, IFF, shared his insights on IT Resilience on *TRT World.*

INDIA FUTURE
FOUNDATION

Contact Us

☎ +91-1244045954, +91-9312580816

Building no. 2731 EP, Sector 57, Golf
Course Ext. Road, Gurugram,
Haryana, India – 122003

✉ helpline@indiafuturefoundation.com

www.indiafuturefoundation.com