INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

IN THE SPOTLIGHT

MODI URGES GLOBAL FRAMEWORK FOR ETHICAL AI, CYBERSECURITY AND DATA PRIVACY

Speaking at the 8th India Mobile Congress, Shri Narendra Modi, Prime Minister of India, stressed on the need for having in place a framework to ensure that artificial intelligence (AI) is ethical, secure, and inclusive. In his speech Mr Modi also emphasised that cybersecurity must be a priority, as no country is isolated from its effects.

The 8th Indian Mobile Congress coincided with the International Telecommunication Union's World Telecommunication Standardization Assembly (WTSA) 2024. The WTSA 2024 was attended by industry leaders from the telecom sector, who advocated for policy reforms aimed at data localisation and measures to combat digital fraud, alongside calls for regulatory clarity on satellite broadband services.

IN THIS NEWSLETTER

IN THE SPOTLIGHT

In his address, Prime Minister Modi urged the WTSA to focus on making telecommunications safe for all. He stated that in an interconnected world, security cannot be an afterthought. He highlighted India's Data Protection Act and the National Cyber Security Strategy as the nation's commitment towards fostering a safe digital environment. He encouraged the WTSA members to develop standards that respect the diversity of nations while addressing ethical AI and data privacy.

Prime Minister Modi also proposed establishing clear global guidelines similar to those in the aviation sector, that ensure safety and security. He emphasised on the importance of collaboration among global institutions to secure a technically robust and ethically sound future.

Shri Jyotiraditya Scindia, Union Minister for Telecommunications, who attended the WTSA stated that the country is working towards setting standards for 6G networks by 2030. He also mentioned the nation's efforts to localize and manufacture chips for the telecom sector.

As India's digital infrastructure evolves, leaders from the telecom sector called for reforms ensuring critical data localization and support for AI and satellite services. Shri Akash Ambani, chairman of Reliance Jio Infocomm, urged the government to expedite updates to the data centre policy to keep critical data within Indian borders.

Shri Sunil Bharti Mittal, chairman, Bharti Enterprises advocated for funding telecom companies via the Universal Services Obligation Fund to expand satellite services. He insisted that satellite companies serving urban customers adhere to the same regulatory standards as telecom operators.

With the new Indian telecom law allowing direct spectrum allocation for satellite broadband services, Mittal emphasised on the nationwide rollout of 5G networks. Kumar Mangalam Birla, chairman, Vodafone Idea highlighted the importance of addressing rising spam, fraud and phishing scams as mobile networks expand.

ANNUAL GLOBAL CYBER-ATTACKS DOUBLE

A recent report from QBE Insurance Group, --*Connected Business: Digital Dependency Fuelling Risk*— reveals that the annual number of disruptive and destructive cyber-attacks globally surged by 105 per cent since 2020. This year alone, in 2024, the number of strategically significant attacks is projected to reach 211, which is a substantial increase from 103 in 2020.

The report cites examples like the NotPetya cyber-attack, which caused extensive infections across Europe, North America and the Asia-Pacific region, resulting in an estimated $10 billion in damages. Unlike routine data breaches or device compromises, these large-scale attacks are fewer in number but far more impactful.

In another major incident on 19 July 2024, the failure of CrowdStrike's Falcon Sensor led to an estimated $5.4 billion in damages for Fortune 500 companies and $25 billion in lost share value. Following this disruption, cybercriminals exploited the situation through phishing campaigns that were aimed at stealing data and extorting victims, underscoring organisations' vulnerabilities during such events.

The report further highlights that cyber incidents are significantly underreported. An analysis conducted by QBE in the United Kingdom found that 69 per cent of medium to large businesses experienced disruptions from cyber-events over the past year. Additionally, 78 per cent of companies expressed concerns over potential cyber threats, with over half of the surveyed companies, anticipating a cyber event within the following year. However, a notable gap in readiness remains: 36 per cent of businesses do not have an incident response plan and 43 per cent lack cyber insurance.

In response to incidents like the CrowdStrike event, 57 per cent of businesses indicated plans to purchase or expand their cyber insurance coverage. The report also noted an emerging reliance on Artificial Intelligence (AI) in cybersecurity, with 32 per cent of surveyed businesses believing AI will enhance their cyber defence capabilities. However, 15 per cent of respondents expressed concerns that AI could amplify cyber risks by enabling more rapid and widespread attacks.

CLOUDFLARE MITIGATES RECORD-BREAKING 3.8 TBPS DDOS ATTACK

On 3rd October 2024, Cloudflare successfully thwarted the most significant Distributed Denial of Service (DDoS) attack ever recorded, with a peak of 3.8 terabits per second (Tbps) and a packet rate of 340 million packets per second (Pps). This unprecedented cyber-attack represents a significant escalation in cybercriminal capabilities, underscoring both the evolving threat landscape and advancements in cybersecurity defences.

The attack lasted approximately 65 seconds and was part of a prolonged campaign targeting multiple industries, including financial services, telecommunications, and Internet providers. The perpetrators utilized Layer 3/4 protocols to flood network bandwidth and overwhelm resources, disrupting legitimate users attempting to access services.

Cloudflare's global network infrastructure, structured on an anycast architecture, was critical in dispersing the attack load across multiple data centres worldwide. This setup prevented any single point from becoming a bottleneck, effectively managing and neutralizing the attack's impact. Cloudflare also employed advanced tools such as eXpress Data Path (XDP) and extended Berkeley Packet Filter (eBPF), enabling rapid packet processing without depleting CPU resources.

The attack was orchestrated mainly using compromised devices, such as MikroTik and ASUS home routers, which were transformed into a botnet and used to generate high volumes of malicious traffic. The botnet traffic predominantly employed UDP on fixed ports from various regions, including Vietnam, Russia, Brazil, Spain, and the United States of America.

This event highlights significant cybersecurity vulnerabilities, especially for organizations relying on less robust protection solutions. Cloudflare's HTTP reverse proxy users benefited from automatic protection, but other properties not equipped with similarly resilient measures remain at risk.

To address growing cyber threats, cybersecurity firms are advancing defence mechanisms. Cloudflare integrates machine learning for traffic profiling and leverages real-time threat intelligence, which adaptively mitigates abnormal activities. The deployment of AI and machine learning in cybersecurity frameworks is increasingly essential to combat the scale and sophistication of modern cyber threats, enabling the rapid identification and neutralisation of complex attack patterns.

This record-breaking incident underscores the importance of robust cybersecurity infrastructure to counteract hyper-volumetric attacks and protect against the growing sophistication of cybercrime.

OPENAI BLOCKS OVER 20 GLOBAL CYBERCRIME AND DISINFORMATION CAMPAIGNS

On 10th October 2024, OpenAI revealed that it had disrupted more than 20 malicious operations globally, thwarting cybercriminals and deceptive networks attempting to misuse its platform for cybercrime and disinformation. These illicit activities included debugging malware, generating content for fraudulent websites, crafting biographies for fake social media profiles, and creating AI-generated images for accounts on platforms like X (formerly Twitter).

OpenAI stated that while some threat actors are experimenting with AI models, there is no evidence that these attempts have led to significant advancements in malware creation or viral audience building. Efforts to influence elections in the U.S., Rwanda, India and the European Union were disrupted. However, these operations failed to attract notable engagement or sustained followers.

Among the highlighted cases was *SweetSpecter*, a suspected China-based adversary using AI for reconnaissance, scripting support, and anomaly detection evasion. Another group, *Cyber Av3ngers*, linked to Iran's Islamic Revolutionary Guard Corps, used AI to research programmable logic controllers. Additionally, *Storm-0817,* an Iranian threat actor, exploited OpenAI's models to debug Android malware and scrape profiles on Instagram.

OpenAI also blocked two influence networks, *A2Z* and *Stop News*, that posted content across websites and social media in English and French. Stop News notably employed DALL-E-generated cartoon-style images to enhance engagement. Additional networks like *Bet Bot* and *Corrupt Comment* misused OpenAI's API for conversations on X, directing users to gambling sites and posting manufactured comments.

The disclosure follows OpenAI's recent ban on accounts connected to *Storm-2035*, an Iranian influence operation targeting the U.S. presidential election. As threat actors refine AI use, cybersecurity firms warn of potential abuse, such as generating microtargeted disinformation through emails and campaign sites allowing misinformation to be scaled and automated with precision.

NORTH KOREAN APT37 EXPLOITS MICROSOFT ZERO-DAY IN 'CODE-ON-TOAST' NO-CLICK ATTACKS

On 21st October 2024, cybersecurity researchers revealed that the North Korea-backed group APT37 (also known as RedAnt, RedEyes, ScarCruft, and Group123) exploited a zero-day vulnerability in Microsoft's Internet Explorer, using it to launch a no-click supply chain attack on South Korean targets. Dubbed "Code-on-Toast," the attack leveraged a Toast ad pop-up feature commonly found in free software installations to deliver data-stealing malware.

Despite Internet Explorer's end of life in 2022, the vulnerability (CVE-2024-38178) remained exploitable in specific applications using IE-based WebView to display ad content. AhnLab Security Intelligence Center (ASEC) reported that APT37 compromised an advertising agency's network, allowing them to inject malicious code into the Toast ad delivery scripts. This allowed the ad scripts to deliver malware, specifically the RokRAT trojan, without user interaction, marking it as a zero-click attack.

The malware, once deployed, enabled remote command execution and persistence through Ruby scripting, with command-and-control managed via a commercial cloud server. While the campaign had the potential for significant harm, early detection limited its impact. AhnLab noted that preventive security measures were also implemented for other Toast programmes before Microsoft issued a patch in its August Patch Tuesday update.

APT37's use of a legacy vulnerability in IE raises concerns about older application components remaining unpatched and susceptible to exploitation. As North Korean threat actors advance in cyber tactics, experts urge users to keep systems updated and recommend that software developers avoid insecure development libraries and modules to mitigate such threats.

IRAN'S APT34 USES MICROSOFT EXCHANGE ZERO-DAY TO SPY ON GOVERNMENT IN THE GULF

On 17th October 2024, reports surfaced of intensified espionage by Iranian threat actor APT34, targeting government agencies in Gulf states, especially in the United Arab Emirates (UAE). APT34, also known as Earth Simnavaz, OilRig, MuddyWater and other aliases, is associated with Iran's Ministry of Intelligence and Security (MOIS). Known for sophisticated attacks on critical infrastructure and high-value targets across industries, APT34 has recently leveraged a new backdoor, "StealHook," exploiting Microsoft Exchange servers to exfiltrate sensitive government data.

According to Trend Micro, an American-Japanese cyber security software company, APT34's recent espionage activity starts with web shell deployment on vulnerable servers. These shells enable the group to execute PowerShell code and facilitate data transfer, which includes tools like ngrok for command-and-control (C2) tunnelling, bypassing security controls to reach a network's Domain Controller.

The threat group has also exploited CVE-2024-30088, a critical vulnerability in multiple Windows versions, which grants system-level privileges on affected machines. Though patched in June 2024, APT34 continues to leverage this exploit alongside a malicious DLL registered as a Windows password filter, intercepting plaintext passwords.

APT34's signature tactic involves StealHook, which allows unauthorized access to Microsoft Exchange servers. This backdoor exploits domain credentials to exfiltrate stolen data through email attachments, a strategy known to evade detection. The group has also used Exchange servers to execute follow-on attacks via phishing emails, potentially compromising multiple organizations through inter-organizational trust relationships.

APT34's advanced methods underscore the need for governments in the Gulf region to enhance security protocols, particularly regarding data exfiltration defences, secure password policies and vulnerability patching in Microsoft Exchange systems.

CHINESE HACKERS INFILTRATE MAJOR AMERICAN TELECOM FIRMS

A group of Chinese hackers gained unauthorised access to several major US telecommunications companies, allegedly in search of sensitive information related to national security. The report by CNN, citing multiple sources, named US broadband and Internet providers AT&T, Verizon, and Lumen among the primary targets of these cyber-attacks.

As central nodes for Internet and phone communications, telecommunications companies manage substantial caller and user data, making them attractive targets for cyber infiltration. The Embassy of China in Washington, DC, rejected these allegations of state-backed hacking, labelling the claims as “distortions of fact.”

The matter has drawn attention at the highest levels within the US Government. Key officials have briefed House and Senate intelligence committee members on this security breach, with investigative support from cybersecurity experts at Microsoft and Mandiant, a Google-owned firm. Experts described the hacker group in the cybersecurity community as "Salt Typhoon," exceptionally skilled and persistent in their infiltration techniques.

The recent attacks emerge amid heightened tensions between Washington and Beijing over cyber espionage and broader national security concerns. Chinese President Xi Jinping assured the then US President Joe Biden that China would not interfere in the domestic affairs of the USA, including the 2024 presidential election. Nevertheless, the ongoing cybersecurity threats underscore the fragile digital relations between the two nations.

According to the Federal Bureau of Investigation’s Director Christopher Wray, Chinese hackers have repeatedly posed threats to critical infrastructure across the US and even across the globe. Prominent think tanks like the Center for Strategic and International Studies have consistently emphasised cyber-attack risks to global digital infrastructure and other essential systems across various sectors.

SOPHOS ANNOUNCES ACQUISITION OF SECUREWORKS

On 21st October 2024, Sophos, a global leader in cybersecurity solutions, announced its definitive agreement to acquire Secureworks, a cybersecurity firm recognised for developing Taegis, a SaaS-based open platform for Managed Detection and Response (MDR) and Extended Detection and Response (XDR). The acquisition will advance the cybersecurity capabilities offered to organisations worldwide, reinforcing both companies' shared mission to build a safer digital landscape.

The integration will enhance Sophos' existing MDR capabilities by merging with the Taegis platform, which leverages over two decades of Secureworks' expertise in detection data, security operations, and threat intelligence. Sophos aims to deliver advanced MDR and XDR solutions by combining their resources to create a more comprehensive cybersecurity portfolio.

Beyond the Taegis platform, Sophos plans to incorporate additional technologies from Secureworks, including Identity Threat Detection and Response (ITDR), next-generation Security Information and Event Management (SIEM) capabilities, Operational Technology (OT) security, and enhanced vulnerability risk prioritisation. These additions are expected to streamline customer threat detection, investigation, and response processes, optimising visibility across native and third-party tools and maximising customer return on investment.

With both organisations prioritising partnership-based growth, the merger is anticipated to increase customer engagement, generate more value for channel partners, and strengthen the security community. The transaction will be finalised in early 2025, pending customary closing conditions. Until then, both companies will maintain their operations independently, ensuring continued support for their clients' cybersecurity needs.

IIT-MADRAS INAUGURATES CYSTAR FOR CUTTING-EDGE CYBERSECURITY RESEARCH

The Indian Institute of Technology-Madras (IIT-M) has inaugurated the Centre for Cybersecurity, Trust, and Reliability (CyStar), a research hub dedicated to advancing India's fundamental and applied cybersecurity research. CyStar aims to bolster cybersecurity across critical national infrastructure and sectors, including finance, healthcare, automotive, and electronics.

CyStar's research agenda spans emerging fields such as blockchain, artificial intelligence security, cryptography, quantum security, and Internet of Things (IoT) security. The centre is positioned to drive innovation through its research and educational initiatives, pushing the boundaries of cybersecurity in India.

CyStar, supported by the Ministry of Electronics and Information Technology and Ministry of Education, will collaborate globally and locally with academia, industry, and research institutions as well as forge partnerships with companies and banks. Such collaborations aims to prepare students, professionals, and researchers to address complex cybersecurity challenges with expertise.

The centre's comprehensive strategy will address cybersecurity risks driven by artificial intelligence and post-quantum technologies, focusing on fortifying critical infrastructure and delivering a robust defence against sophisticated cyber threats.

CYBERSECURITY EXECUTIVES CALL FOR STRONGER GOVERNMENT POLICIES

As the cybersecurity threat landscape in India grows increasingly complex due to the rise of artificial intelligence (AI), industry leaders are urging the government to modernise existing frameworks and policies to bolster the nation's cyber resilience. This was the focal point of a recent panel discussion organised by Microsoft India entitled 'Cybersecurity in the Age of AI.'

In the panel discussion, executives fromorganisations like KPMG, Wipro and GMR Group emphasised on the necessity of establishing a dedicated ministry for cybersecurity to prioritise the nation's cyber defence. They stressed that as India becomes more digitised, enhancing cybersecurity should be a top priority for the government to ensure the safety of its citizens and economic stability.

The Role of AI in Cybersecurity

While the rise of generative AI has led to a rise in malicious activities unleashed by threat actors, which has led to tech companies like Microsoft increasingly employing AI to enhance security measures for their products and services. Microsoft introduced Copilot, in 2023, an AI-driven solution. This tool empowers cybersecurity defenders to shift from reactive to proactive strategies, allowing them to respond 26 per cent faster and 35 per cent more accurately to security incidents.

KPMG executives highlighted the benefits of AI in cybersecurity, particularly its ability to improve the signal-to-noise ratio for security teams inundated with alerts. AI can help filter out irrelevant information, enabling teams to concentrate on significant threats. Additionally, the potential of generative AI to simulate more sophisticated phishing attacks was noted as a means to enhance training for security personnel.

AI can also streamline the work of security analysts by enabling them to interact with AI tools conversationally, saving significant time when managing cybersecurity incidents.

Strengthening Cyber Resilience

Representatives from Wipro emphasized on the importance of awareness in fostering cyber resilience, calling for creating frameworks that build trust in security systems and promote the safe adoption of digital technologies. An updated version of India's National Cyber Security Policy (NCSP), which is in the process of development, is crucial for this effort.

To address the shortage of cybersecurity professionals in India, there is a suggestion to initiate training programmes at the university level. With over 5,25,000 villages in the country, ensuring everyone has access to such training requires significant government support.

The panellists also discussed the need for collaboration among cybersecurity defenders, although challenges remain due to the different motivations of attackers and defenders.

Microsoft's Renewed Focus on Cybersecurity

Following critical reviews of its security culture, Microsoft launched the Secure Future Initiative (SFI), employing over 34,000 engineers to enhance its cybersecurity posture. This initiative comes in light of a significant outage experienced by Microsoft Windows systems in July 2024, which disrupted critical infrastructure globally.

In summary, the call for more robust government policies, the role of AI in cybersecurity, and the emphasis on collaboration and training underscore the pressing need for enhanced cybersecurity measures as digital threats evolve.

CYBERSECURITY FIRM ARCTIC WOLF OPENS FIRST INDIA GCC IN BENGALURU

US-based cybersecurity firm Arctic Wolf has announced the opening of its first Global Capability Centre (GCC) in Bengaluru, India. The company plans to recruit 150 employees by mid-2025, focusing primarily on roles in core research and development areas such as threat intelligence and artificial intelligence (AI).

Bengaluru, recognised as a global technology and cybersecurity talent hub, will be crucial for driving innovation and enhancing Arctic Wolf's security operations platform. The establishment of this centre is expected to provide the firm with around-the-clock development capabilities and improved proximity to clients in the Asia-Pacific (APAC) region.

The new GCC is anticipated to create numerous job opportunities, attracting top-tier talent from India's IT and cybersecurity sectors.

RRU TO TRAIN 30 COPS AS 'CYBER COMMANDOS'

The Rashtriya Raksha University (RRU) will train 30 police officers, including four women, as 'cyber commandos' in a six-month training programme that was inaugurated at the University's campus in Lavad, Gandhinagar. This initiative is a collaboration with the Indian Cyber Crime Coordination Centre under the Ministry of Home Affairs and was announced by Shri Amit Shah, Union Home Minister, Government of India on September 10, according to an official release from the University.

Director General of Police Vikas Sahay, the chief guest at the event, highlighted the significance of establishing such a specialised unit within law enforcement. He drew parallels with historically successful anti-crime units like the Greyhounds, which effectively addressed Naxalism.

The six-month residential programme will provide practical instruction in ethical hacking, digital forensics, threat intelligence, incident response strategies, and other advanced cybersecurity measures. The curriculum will also cover essential topics such as IT fundamentals, cloud computing, cyber laws, and IoT security.

US AND INDIA COLLABORATE TO STRENGTHEN CYBERSECURITY

Prime Minister Narendra Modi's visits to the US in 2023 and 2024 deepened the US-India partnership, with cybersecurity emerging as a central focus in the discussions between the two countries. This partnership between the two countries seeks to foster safer digital environments and resilient critical infrastructure. The White House Briefings reflected a shared commitment to counter cyber threats and protect interconnected systems across nations.

This partnership addresses critical sectors beyond government strategies, including secure telecommunications, defence and energy systems. Through collaborative efforts, the US and India are building robust cybersecurity protocols to enhance global digital stability, benefiting millions worldwide.

Advancing Cybersecurity Research and Technology

The joint cybersecurity foundation established in 2023 has grown into collaborative efforts in quantum encryption and AI-driven defence, essential for protecting sensitive data. Quantum encryption and AI-based systems are crucial for rapid threat detection and maintaining critical infrastructure security, such as power grids and emergency services.

Securing Telecommunications Infrastructure

The US and India's 5G Open RAN project launched in 2023 emphasizes telecommunications security. This project provides mobile networks greater flexibility and protection, reassuring banking, telemedicine, and personal communication users. The upcoming "Rip and Replace" programme also aims to eliminate vulnerable equipment from telecom networks, reducing data breach risks.

Protecting Space Systems from Cyber Threats

The partnership also focuses on safeguarding space systems, crucial for secure satellite communications and planetary defence systems. With India's role in space exploration expanding, the US-India collaboration on cybersecurity ensures safe data transmission for essential technologies impacting global navigation, climate research, and weather forecasting.

Enhancing Defence Technology Resilience

This alliance strengthens military cybersecurity in the defence sector, focusing on cyber-resilient uncrewed aerial vehicles (UAVs) and secure communication channels. These efforts protect national security by deterring cyber threats to critical defence systems.

A Model for Global Cybersecurity Collaboration

The US-India cybersecurity partnership demonstrates how international collaboration can address cyber threats, setting a standard for secure digital infrastructure worldwide. As the world becomes increasingly interconnected, this alliance reassures citizens of both nations that the digital services they depend on will remain safe and resilient against cyber risks.

This partnership builds a secure foundation for future digital innovations, prioritising security and privacy for a safer global digital landscape.

IFF IN THE MEDIA

Kanishk Gaur, Founder & CEO, IFF, discussed the new Technology Neuralink and Ethical AI on *News Nine*.

Kanishk Gaur, Founder & CEO, IFF, shared his knowledge of Data Protection and Online Scams on *NDTV*.

Kanishk Gaur, Founder & CEO, IFF, shared his insights on "Bomb Scare: Misuse of Social Media and VPNs" on *News Nine*.

Kanishk Gaur, Founder & CEO, IFF, talked about Digital Safety on *DD National*.

Kanishk Gaur, Founder & CEO, IFF, talked about Cyber Slavery Scams on *News18*.

Kanishk Gaur, Founder & CEO, IFF, talked about Digital Arrest on *India Today*.

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