INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

IN THE SPOTLIGHT

INDIA ADVOCATES FOR GLOBAL ANTI-TERRORISM TREATIES TO ADDRESS CYBERCRIMES

On 20 June 2024, India called for the application of global anti-terrorism treaties in the cyber domain during a UN Security Council meeting, in New York. The meeting, held under the agenda item "Maintenance of International Peace and Security," aimed to address the evolving threats in cyberspace.

India highlighted the inadequacy of current international laws in supporting responses to cyberattacks. As a country that has experienced terrorism for several decades, India underscored its awareness about the severe nature of cyberterrorism. The Indian representative, at the UN, emphasized on the importance of classifying cyber threats—such as attacks on critical infrastructure, information and financial systems, and government networks—as terror attacks. These cyber-threats have the potential to jeopardize national security and undermine global stability and cooperation.

IN THIS NEWSLETTER

India pointed out that terrorists are exploiting cyber space for violence, radicalizing youth recruitment and training, and finding funding methods through virtual assets and cryptocurrency. The representative mentioned the frequent occurrences of cryptocurrency heists, data hijacking, deep fakes, misinformation, and incitements. The potential of artificial intelligence to scale cyberattacks was also noted. The integrity and security of ICT products, which form the building blocks of cyberspace, are being compromised by nefarious acts, leading to a loss of trust in global ICT supply chains and creating potential flashpoints between states. These acts are often committed by state-sponsored actors, non-state actors, and transnational crime networks.

India called for global cooperation in harmonizing cybersecurity benchmarks, best practices, and regulations. The representative emphasized on the necessity of multi-stakeholder collaboration to understand and respond to emerging threats in cyberspace.

The UN Cyber Crime Treaty, under discussion by the UN Ad-Hoc Committee, aims to create an international convention to tackle cybercrimes. India has actively participated in these discussions, proposing a '24×7 global communication network' to combat phishing. This network would allow law enforcement agencies to swiftly render phishing links inaccessible and identify the abused IT resources and malicious actors. The proposed communication channel would facilitate information exchange between global law enforcement agencies, enabling prompt action against cyber threats in accordance with domestic law.

By advocating for these measures, India aims to enhance global cybersecurity resilience and ensure a secure digital environment.

FBI TAKES DOWN ARMY OF 'ZOMBIE' COMPUTERS

On 19 June 2024, the FBI dismantled a network of 19 million computers infected with malware, marking the world's largest botnet takedown. This network, comprised of 'zombie devices,' that facilitated various crimes, including financial fraud and identity theft, across nearly 200 countries.

The FBI described the operation as something "ripped from a screenplay," revealing that the botnet, known as "911 S5," enabled its operators to commit crimes using the hijacked computers. The network's alleged operator used the proceeds to purchase luxury items and properties worldwide.

Botnets are created when cybercriminals use malware like Trojans to breach users' computers and Internet of Things (IoT) devices. The malware is often hidden in email attachments or links, tricking users into downloading it. In the case of 911 S5, residential IP addresses were compromised through pirated software or VPN programmes.

In this case the criminals remotely managed the infected machines, transforming them into a "zombie army." The botnet's activities included launching denial-of-service attacks and phishing emails to steal credentials. The FBI stated that the 911 S5 network was used to target pandemic relief programmes, resulting in fraudulent losses amounting to over $5.9 billion.

Cybercrime is on the rise, with predictions estimating the global cost of cybercrime to reach almost $14 trillion by 2028. Microsoft identifies password theft, ransomware, and phishing as top cyber threats.

Efforts to combat cybercrime face challenges, including a global shortage of nearly 4 million cyber professionals. The lack of clear career paths, outdated training and costly certifications are barriers to entering the cybersecurity field. The World Economic Forum's Centre for Cybersecurity aims to drive public-private action against cybercrime and bridge the cyber-skills gap.

G7 TO DEVELOP CYBERSECURITY FRAMEWORK FOR THE ENERGY SECTOR

In a recent development the G7 nations announced plans to develop a collective cybersecurity framework for operational technologies in energy systems. This initiative targets manufacturers and operators, aiming to bolster cybersecurity globally in critical technologies like electricity, oil, and natural gas systems.

Shri Jake Sullivan, US National Security Advisor, revealed this agreement at the G7 Leaders' Summit in Apulia, Italy on 18 June 2024. The framework's goal is to strengthen cybersecurity in the global supply chain, thereby ensuring the protection and resilience of energy systems against continuous cyberattacks.

Shri Sullivan emphasised on the importance of cybersecurity as new digital clean energy technologies are integrated, highlighting the importance of preventing potential disruptions or destruction in services.

The G7, an intergovernmental political and economic forum, includes countries like Canada, France, Germany, Italy, Japan, the United Kingdom and the United States of America.

US Releases Energy Supply Chain Security Principles

With the G7's announcement, the US Department of Energy (DOE) has taken a proactive step towards ensuring robust cybersecurity across global supply chains. The release of the new Supply Chain Cybersecurity Principles is a reassuring sign for the future of energy automation and industrial control systems (ICS).

The DOE highlighted the inherent complexity of energy ICS, noting that a single product or system could contain hundreds of subcomponents sourced from suppliers and manufacturers worldwide. This complexity creates a dense web of stakeholders, making security a shared responsibility among engineers, manufacturers, integrators, service providers, and system operators.

The principles condense various international cybersecurity regulations, frameworks, and guidance into 20 high-level objectives that energy suppliers and manufacturers can use to align best practices in the cybersecurity supply chain. These objectives include secure development and implementation, lifecycle support and management, and proactive vulnerability management.

Several prominent energy suppliers and manufacturers, including GE Vernova, Schneider Electric, Hitachi Energy, Honeywell, Schweitzer Engineering Laboratories, Rockwell Automation, Siemens, and Siemens Energy, have already expressed their support for these principles.

Building on the US Government's Supply Chain Security Initiatives

The G7 agreement builds on US Government's efforts to strengthen critical supply chains for economic and national security. On 14 June 2024, President Joe Biden issued an Executive Order on the White House Council on Supply Chain Resilience. This order established the Council's role in coordinating and promoting federal efforts to enhance long-term supply chain resilience.

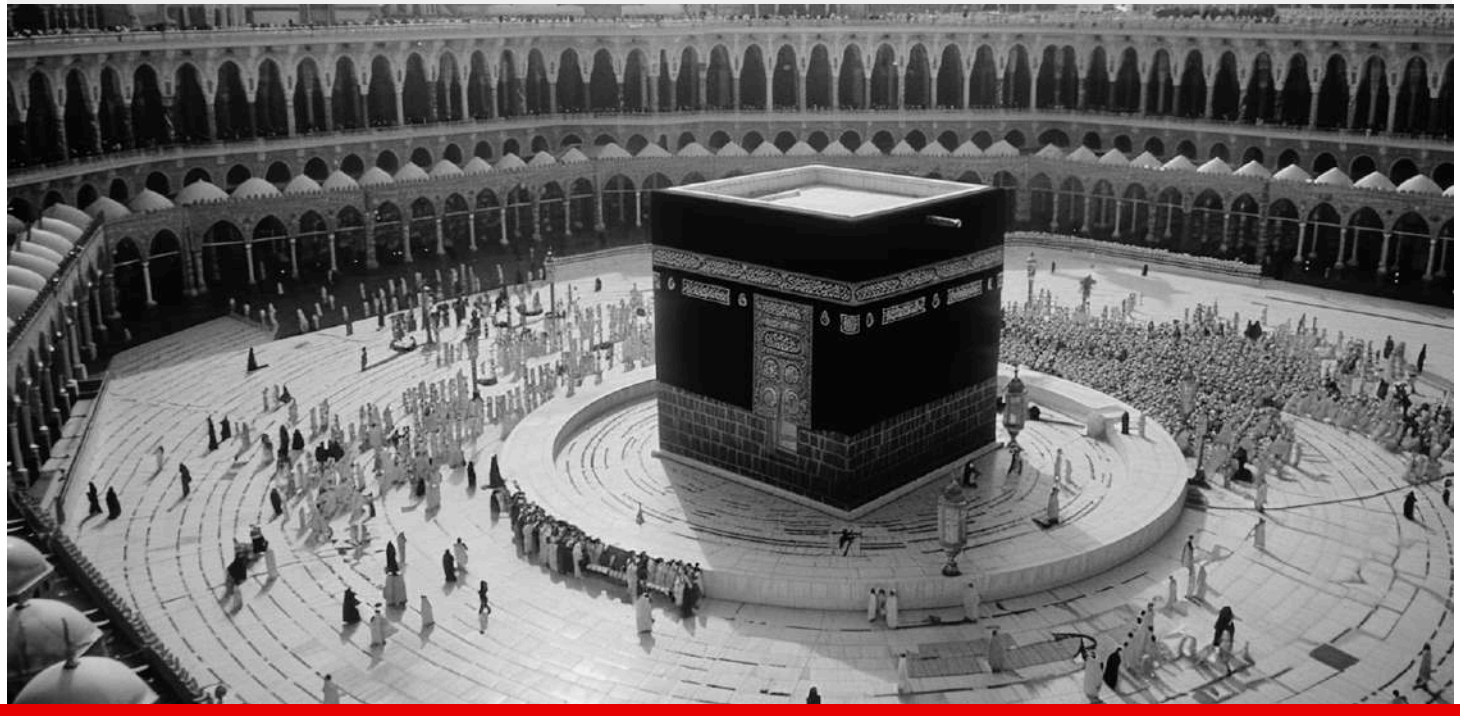
GOVERNMENTS, BUSINESSES TIGHTEN CYBERSECURITY AROUND HAJJ SEASON

As the final month of the Islamic calendar, Dhu al-Hijjah, began on 7 June 2024, millions of Muslims prepared for the Hajj pilgrimage. This period also marks an increased risk for cyberattacks, as cybercriminals and espionage actors exploit reduced vigilance and limited staffing.

While cyberattacks tend to decrease slightly during the week of the Hajj pilgrimage, organisations in Saudi Arabia and other countries with large Muslim populations often see a rise in attacks. These attacks target various sectors, including banks and e-commerce sites, focusing on data theft and denial-of-service attacks.

On 3 June 2024, cyber threat actors announced a data leak on an underground forum, claiming to contain the personal information of 168 million users from "The Hajj and Pilgrimage Organization in Iran," according to cybersecurity firm Kaspersky.

Cyber attackers see an opportunity to exploit pilgrims and security teams' reduced resources, making businesses and government agencies more vulnerable. During this period companies in the Middle East and other regions should exert extra caution during holiday seasons such as the Hajj.



The Hajj pilgrimage begins on the eighth day of the Islamic month and lasts four to six days. It sees nearly a week of religious holidays for the entire Middle East and an estimated 2 billion Muslims worldwide. Cyberattacks can drop by up to 30 per cent during this period but quickly rebound. In 2022, cyberattacks doubled to more than 2 million during Dhu al-Hijjah, the month starting with the appearance of the new crescent moon.

Cyber threats linked to the Hajj pilgrimage often begin early in the year, with cybercriminals targeting Muslims planning to travel to Saudi Arabia. These threats include fake travel agencies, social media scams, and fraudulent online registration sites. In response, Saudi Arabia's Ministry of Hajj and Umrah launched the government platform Nusuk, connecting prospective pilgrims with legitimate operators and significantly reducing fraud.

Advanced threat actors also use Hajj-related messages to lure employees into opening malicious links and attachments. From January to May 2024, the India-linked threat group Sidewinder, also known as Rattlesnake, targeted users in Asia and Africa with Hajj-related emails.

CDK GLOBAL INVESTIGATES CYBER INCIDENT, BRIEFLY SHUTS DOWN ALL SYSTEMS

On 19 June 2024, CDK Global, a retail technology and software provider, based in Austin, United States, reported a cyber incident that led to the proactive shutdown of all its systems. CDK Global, which supplies software to car dealerships, has since restored its core dealer management system and digital retailing solutions. The company is conducting extensive tests on other applications and consulting with external third-party experts to ensure system integrity before returning them online.

The systems first went down at around 2:00 a.m. EDT (0600 GMT), with some functions returning online by the afternoon. CDK Global assured of continuous updates as they worked to restore all affected applications. The company was acquired by Brookfield Business Partners in April 2022 for $6.41 billion.

CHINESE AND NORTH KOREAN HACKERS TARGET GLOBAL INFRASTRUCTURE

On 26 June 2024, cybersecurity firms reported that threat actors linked to China and North Korea have conducted ransomware and data encryption attacks on critical infrastructure, at the global level between 2021 and 2023.

One of the attackers involved in such attacks was ChamelGang (aka CamoFei), was responsible for targeting entities such as the All India Institute of Medical Sciences (AIIMS) and the Presidency of Brazil in 2022, using CatB ransomware. In 2023, they attacked a government entity in East Asia and an aviation organisation in the Indian subcontinent.
Cybersecurity researchers noted a troubling trend of cyber espionage actors using ransomware to destroy evidence and achieve financial gain, disruption, and cover-up operations. This tactic allows attackers to misattribute their activities or remove traces that could alert defenders.

ChamelGang, first documented in 2021, is believed to be a China-nexus group with motivations including intelligence gathering, data theft, financial gain, denial-of-service (DoS) attacks, and information operations. The group uses various tools, such as BeaconLoader and Cobalt Strike, and backdoors like AukDoor and DoorMe, alongside the CatB ransomware strain.

In 2023, ChamelGang updated BeaconLoader to deliver Cobalt Strike for reconnaissance and post-exploitation activities, including dropping additional tools and exfiltrating the NTDS. dit database file. Their custom malware, such as DoorMe and MGDrive, has also been linked to other Chinese threat groups like REF2924 and Storm Cloud, indicating a possible shared digital quartermaster.

The second set of intrusions involved tools like Jetico BestCrypt and Microsoft BitLocker, targeting industry sectors in North America, South America, and Europe. Thirty-seven organisations, mainly in the U.S. manufacturing sector, were affected. These attacks showed tactics consistent with Chinese hacking group APT41 and North Korean actor Andariel, using tools like the China Chopper web shell and the DTrack backdoor.

Cybersecurity researchers stated that while there were no concurrent signs of tools from Chinese and North Korean APT groups in the same environments, the activities observed might be part of a broader cybercriminal scheme. This could indicate that nation-state actors sometimes engage in financially motivated attacks.

The use of ransomware by cyber espionage groups blurs the lines between cybercrime and state-sponsored espionage, offering strategic and operational advantages. This allows adversarial nations to claim plausible deniability by attributing actions to independent cybercriminals rather than state-sponsored entities.

SNOWBLIND TAMPERING TECHNIQUE MAY DRIVE ANDROID USERS ADRIFT

Southeast Asian hackers have exploited a core Android security feature to perform tampering using a method with no apparent fix. This new malware, named "Snowblind," targets at least one banking application in Southeast Asia by severing the link between the kernel and the application. It abuses the Linux security feature "seccomp" to trap and modify system calls in transit, isolating an application from the protocols and information it needs to detect tampering.

The Android Anti-Tampering Cat & Mouse Game

A report by Promon, a firm working in the realm of application security, on Snowblind details how attackers usually undermine Android devices by tricking users into granting accessibility permissions. Developers counteract this by querying the operating system for untrusted accessibility services and reacting accordingly. Attackers then repackage legitimate applications with malicious code, which developers counter with code obfuscation and proactive file reviews.

Snowblind's New Tactic

Snowblind employs a new tactic by focusing on the seccomp security feature. This feature is used by containerisation technologies and Chromium browsers to sandbox applications, allowing or blocking calls to the operating system. Snowblind repackages an application with a library loaded before any anti-tampering mechanisms can run. This library traps system calls like "open()" and modifies them to point to an unmodified version of the application.

No Perfect Solutions

This technique allows a banking Trojan to use accessibility services to steal credentials, intercept 2FA codes, and turn off application security features. Snowblind's strategy can theoretically be used in cloud environments, Chromium browsers, and any system relying on seccomp.

There isn't an apparent seccomp-oriented fix, as it’s integral to many applications. Google and its customers should focus on preventing maliciously repackaged applications from being downloaded. In Southeast Asia, these applications often spread outside official app stores via social engineering.

Google responded that they were aware of Snowblind before the report by Promon. The company maintained that no applications containing this malware are found on Google Play. Android users are protected by Google Play Protect, which can warn users or block applications exhibiting malicious behaviour, even outside the Play Store.

77% OF INDIAN COMPANIES WITNESS SURGE IN CYBERSECURITY INCIDENTS

Grant Thornton Bharat's latest 'Financial & Cyber Fraud Survey' reveals that 77 per cent of Indian organisations have seen a rise in fraudulent activities post-pandemic. The survey highlights significant challenges in the current business landscape, with cyber incidents accounting for 64 per cent of these frauds.

Emerging threats are increasingly prevalent, with 71 per cent of organisations reporting business email compromise, 65 per cent having experienced social engineering attacks and 54 per cent have delath with instances of identity theft. The shift from onsite to remote work and the lack of stringent internal controls have been identified as key factors contributing to this surge, in cyberattacks.

However, efforts are being made to counter this rising trend, especially with the growing awareness among organisations regarding fraud prevention. What is heartening is that companies now prioritise cybersecurity and anti-fraud technologies. There is however, much room for improvement, especially with regards adoption of artificial intelligence (AI) and machine learning (ML) by organisation in combating cyberattacks.

The survey also reveals the financial impact of these fraudulent activities, with one-fourth of organizations having suffered losses of INR 1 crore and more. The sad part is that of the organisations surveyed three-fourths of them have faced financial damages exceeding INR 5 crore. Over three out of five organisations surveyed support a collaborative approach with forensic professionals to investigate fraud.

The most affected industries include technology, media and telecommunications (58 per cent), financial services (51 per cent), and manufacturing (46 per cent). The survey showed that 84 per cent of organisations that encountered instances of fraud stressed on the pivotal role of an external perpetrator alone or colluding individuals from the organisations, in execution of such attacks.

What's heartening to know is that post COVID-19, as per the survey, 73 per cent of organisations have enhanced their governance and compliance frameworks, 63 per cent have implemented awareness training for employees, third parties, and customers, and 62 per cent are conducting continuous control assessments of high-risk areas. By embracing tailored solutions and advanced technologies, organisations can strengthen internal controls, foster a culture of awareness and promote trust and resilience in today's complex market.

MASTERCARD AND CERT-IN COLLABORATE TO ENHANCE CYBERSECURITY

On 20 June 2024, CERT-In and Mastercard signed a Memorandum of Understanding (MoU) to bolster cybersecurity in the financial sector through collaboration and information sharing. The Indian Computer Emergency Response Team (CERT-In) and Mastercard will utilise their combined expertise to improve cybersecurity incident response, capacity building, and cyber threat intelligence specifically for the financial sector.

CERT-In, India's nodal cybersecurity agency under the Ministry of Electronics and Information Technology (MeitY), is designated as the national agency for incident response under Section 70B of the Information Technology Act, 2000. Through this MoU, CERT-In and Mastercard will conduct training programmes and workshops focused on cyber capacity building, latest market trends and best practices to enhance the cybersecurity of financial sector organisations.

This partnership will also involve sharing relevant cyber threat trends, technical information, threat intelligence, and vulnerability reports to strengthen information security in India's financial sector.

RESECURITY AND CYBER SECURITY ASSOCIATION OF INDIA SIGN MOU

On 25 June 2024, Resecurity, a cybersecurity firm based in the United States of America (USA), signed a Memorandum of Understanding (MoU) with the Cyber Security Association of India (CSAI) to enhance cybersecurity awareness, education, research, and practices in India and across the globe. This agreement aims to foster collaboration and advance cybersecurity initiatives, promoting mutual growth opportunities.

Through this partnership, Resecurity and CSAI will conduct awareness campaigns, educational programmes, and research projects and develop cybersecurity tools and best practices. The collaboration addresses cybersecurity challenges and promotes a secure digital environment in India.

As part of the MoU, the American cybersecurity and risk management solutions firm and CSAI will exchange knowledge, expertise, and information on cybersecurity threats, vulnerabilities, and mitigation strategies. This exchange aims to improve both organisations' cybersecurity posture and resilience.

The partnership will also focus on capacity building by developing and delivering training programmes to strengthen the skills and knowledge of cybersecurity professionals and stakeholders. By investing in education and skill development, Resecurity and CSAI aim to empower individuals and organisations to address cyber threats effectively.

The collaboration aligns with the broader objectives of the Government of India’s Digital India initiative, reinforcing efforts to create a digitally empowered society. By working together, Resecurity and CSAI aim to contribute to India's cybersecurity resilience and promote growth in the cybersecurity domain.

91% OF SECURITY LEADERS BELIEVE AI SET TO OUTPACE SECURITY TEAMS

On 27 June 2024, Bugcrowd – an IT Security Company released its "Inside the Mind of a CISO" report, revealing critical insights from hundreds of security leaders worldwide on AI threats, ethical hacking, and the expertise needed to address the cyber skills gap. The report highlights significant concerns and priorities for Chief Information Security Officers (CISOs) as they navigate the evolving cybersecurity landscape.

Key Findings:

- **AI Threats and Workforce Impact:** Over 90 per cent of security leaders believe that AI already performs better than security professionals or will do so in the very near future. Despite plans to hire more security staff, 70 per cent of the leaders surveyed indicated their intentions to reduce headcount within the next five years due to AI adoption. Additionally, 58 per cent of them view AI's risks as outweighing its potential benefits.

- **Ethical Hacking and Crowdsourced Security:** Due to concerns over use of AI for malicious uses, by attackers 70 per cent of security leaders have turned to crowdsourced security to test their AI defences. Ethical hacking is viewed favourably by 73 per cent of security leaders, with 75 per cent having personal experience in practice. With modern threats becoming more elusive, 89 per cent believe there are more severe threats now than ever.

- **Economic and Hiring Trends:** One in three respondents believe many companies are willing to compromise customer privacy or security to save money. While 87 per cent are currently hiring security staff, 56 per cent reported that their teams are understaffed. Furthermore, only 6 per cent of cybersecurity leaders lack a college degree, with over 80 per cent hold degrees specifically in cybersecurity.

Global Participation and Analysis: The report analysed 209 survey responses from security leaders across North America, South America, Europe, Asia, Australia, and Africa. It focused on individuals with titles such as CISO, CIO, CTO, Head of Security, or VP of Security. The findings provide a detailed look at CISO priorities, common misconceptions, and perceptions of the threat landscape.

INDIA FUTURE FOUNDATION (IFF) HOSTED A DISCUSSION ON AI INNOVATIONS FOR CYBER ASSURANCE

In association with Microsoft, India Future Foundation (IFF) hosted a panel discussion, **"Strengthening Bharat's BFSI: AI Innovations for Cyber Assurance."** The event, held on 7 June 2024 at Taj Lands' End, Mumbai, brought together industry leaders, government officials, and academic experts to discuss the critical role of AI in enhancing cybersecurity from the Banking, Financial Services, and Insurance (BFSI) sector.

The panel was moderated by Mr Kanishk Gaur, Founder and CEO of India Future Foundation. Esteemed speakers included Lt Gen. (Dr) Rajesh Pant (Retd), Chairman, India Future Foundation; Mr Shailendra Thakur, Chief Technology Transform, NPCI Bharat BillPay Ltd.; Mr Hiten Sinha, CISO, Bombay Stock Exchange; Mr Gulshan Narula, Head, Centre of Excellence - Availability and Reliability, ICICI Bank; Captain Manmeet Singh Kapoor, Chief Operating Officer, TCA2I, IIT Bombay and Mr Kaushal Todi, Director, Customer Success, Microsoft.

The discussion explored at integrating AI technologies to enhance the cyber security measures in the BFSI sector. Key topics included the importance of data sovereignty in cloud migration, strategies for successful cloud adoption, and the role of Data Protection Officers (DPOs) in ensuring compliance with new data protection regulations such as the Digital Personal Data Protection Act, 2023.

Lt Gen. (Dr) Rajesh Pant (Retd) emphasised on the significance of data sovereignty, stating, "Data sovereignty is a crucial aspect. It's about where you localise it and who can access and delete it." The panellists discussed the need for robust security measures, including data protection, encryption, and stringent access controls, to safeguard sensitive information and maintain trust in the financial system.

Shri Shailendra Thakur highlighted the evolving threat landscape and the importance of continuous innovation in cybersecurity. He noted, "Our responses, although sufficient till now, need to keep evolving as we face multifaceted challenges from rogue actors in the security domain."

The event also addressed the challenges of cloud adoption, including security and compliance concerns, cost implications, and the skills gap in managing cloud and cybersecurity technologies. Captain Manmeet Singh Kapoor emphasised on the potential for collaboration between industry and academic institutions to develop innovative cybersecurity solutions tailored to India's specific needs.

The panel underscored the importance of a collaborative, multi-layered approach to fortifying Bharat's BFSI sector against cyber threats. The collective insights and recommendations aim to secure and innovate India's financial services, ensuring a resilient digital future.

IFF HOSTED INSIGHTFUL DISCUSSION ON AI ERA PRODUCTIVITY AT DIGITAL HORIZONS 2024

In association with Microsoft, the India Future Foundation (IFF) hosted an insightful discussion on **Digital Horizons: "AI Era Productivity and Collaboration for Public Sector Organisations."** Held on 12 June 2024 at The LaLiT, New Delhi, the event brought together industry leaders, government officials, and academic experts to discuss AI's transformative capabilities in enhancing productivity and collaboration within the public sector.

The panel was moderated by Mr Kanishk Gaur, Founder and CEO, IFF. Esteemed speakers included Dr B.K. Murthy, Former Senior Director (Scientist G) & Group Coordinator (R&D in IT), Ministry of Electronics and Information Technology (MeitY); Prof. (Dr) Shailesh Tiwari, Director, Krishna Engineering College; Col. Sanjeev Relia (Retd), Chief Strategy Officer, Athenian Tech; and Ms Puneet Sawhny, Director-Cloud Solutions, Public Sector, Microsoft India.

The discussion explored the integration of AI and cloud computing solutions to improve productivity and efficiency in government and public sector organisations.

Key topics included leveraging AI for day-to-day service delivery, increasing organisational productivity through AI-driven content creation and summarisation, and streamlining operations with cloud-based document management and communication solutions.

The event also addressed the challenges of AI adoption in the public sector, including integrating AI with legacy systems, the need for robust data governance, and the importance of public awareness and ethical considerations in AI deployment. Prof. (Dr) Shailesh Tiwari emphasised on the need for a uniform framework to bridge the gap between industry and academia, fostering collaboration and resource sharing.

Overall, the panel underscored the importance of a collaborative, multi-layered approach to enhancing productivity and collaboration in the public sector through AI and cloud technologies. The collective insights and recommendations aim to drive innovation, improve efficiency, and ensure responsible and effective AI adoption in public sector organisations.

IFF IN THE MEDIA

Kanishk Gaur, Founder & CEO, IFF, highlights Tesla's appeal for China over India in a discussion with *Mirror Now*

Kanishk Gaur, Founder & CEO, IFF, shared his insights on WhatsApp's encryption dilemma and India's new IT regulation on *News9 Plus*

Kanishk Gaur, Founder & CEO, IFF, shared his insights on "Artificial Intelligence" on *News9 Plus*

Kanishk Gaur, Founder & CEO, IFF, discussed the rising threat of deepfakes on *Mirror Now*

Kanishk Gaur, Founder & CEO, IFF, talked about Online Safety with *NDTV*

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