INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

IN THE SPOTLIGHT

INDIA REACHES TIER 1 IN GLOBAL CYBERSECURITY INDEX 2024

India has reached a significant milestone by achieving Tier 1 status in the Global Cybersecurity Index (GCI) 2024, published by the International Telecommunication Union (ITU). Scoring 98.49 out of 100, India has positioned itself as one of the 'role-modelling' countries, recognised for its strong commitment to cybersecurity on the global stage. India joins 10 other Asia-Pacific countries, including Australia, Japan, and Singapore, in this prestigious category.

The Department of Telecommunications (DoT) played a pivotal role in representing India in the GCI 2024. Shri Jyotiraditya M Scindia, Minister of Communications, hailed this achievement as a "proud moment for Bharat," emphasising that it reflects India's unwavering dedication to strengthening its cybersecurity framework and enhancing the telecom sector's resilience.

IN THIS NEWSLETTER

The GCI 2024 assessed countries across five key pillars: legal, technical, organizational, capacity development and cooperation. India's success is attributed to comprehensive initiatives taken to bolster cyber resilience, establish robust cybercrime laws and develop cybersecurity standards. Sectoral Computer Incident Response Teams (CSIRTs) further contribute to this effort by providing sector-specific technical support.

Education has been at the core of India's strategy, with targeted campaigns promoting cybersecurity awareness across public and private sectors. Integrating cybersecurity education into primary and secondary school curricula has also been crucial in cultivating a knowledgeable and secure digital population.

India's strong performance is further enhanced by international collaborations, bilateral agreements and incentives for research and innovation in cybersecurity. With this achievement, India has set a benchmark for other nations, reinforcing its position as a global leader in cybersecurity.

This accomplishment underscores India's commitment to securing its digital infrastructure and marks a major step in its efforts to strengthen cybersecurity on the global stage.

CYBERATTACK DISRUPTS WI-FI NETWORKS AT MAJOR RAILWAY STATIONS IN THE UK

A cyberattack disrupted public Wi-Fi services at 19 of the United Kingdom's largest railway stations, including key hubs like London Euston, Paddington, Manchester Piccadilly and Birmingham New Street. The breach, which occurred on the evening of 25 September 2024, left the Wi-Fi network inaccessible, with passengers encountering messages about terror attacks in Europe when attempting to connect.

The Wi-Fi service, managed by Telent on behalf of Network Rail, was taken offline immediately after the attack was detected. British Transport Police (BTP) launched a criminal investigation into the incident, with early findings indicating that someone using a legitimate Global Reach administrator account made an unauthorised change to the Wi-Fi homepage. Telent confirmed that the attack originated from this misuse, and that the is under police investigation.

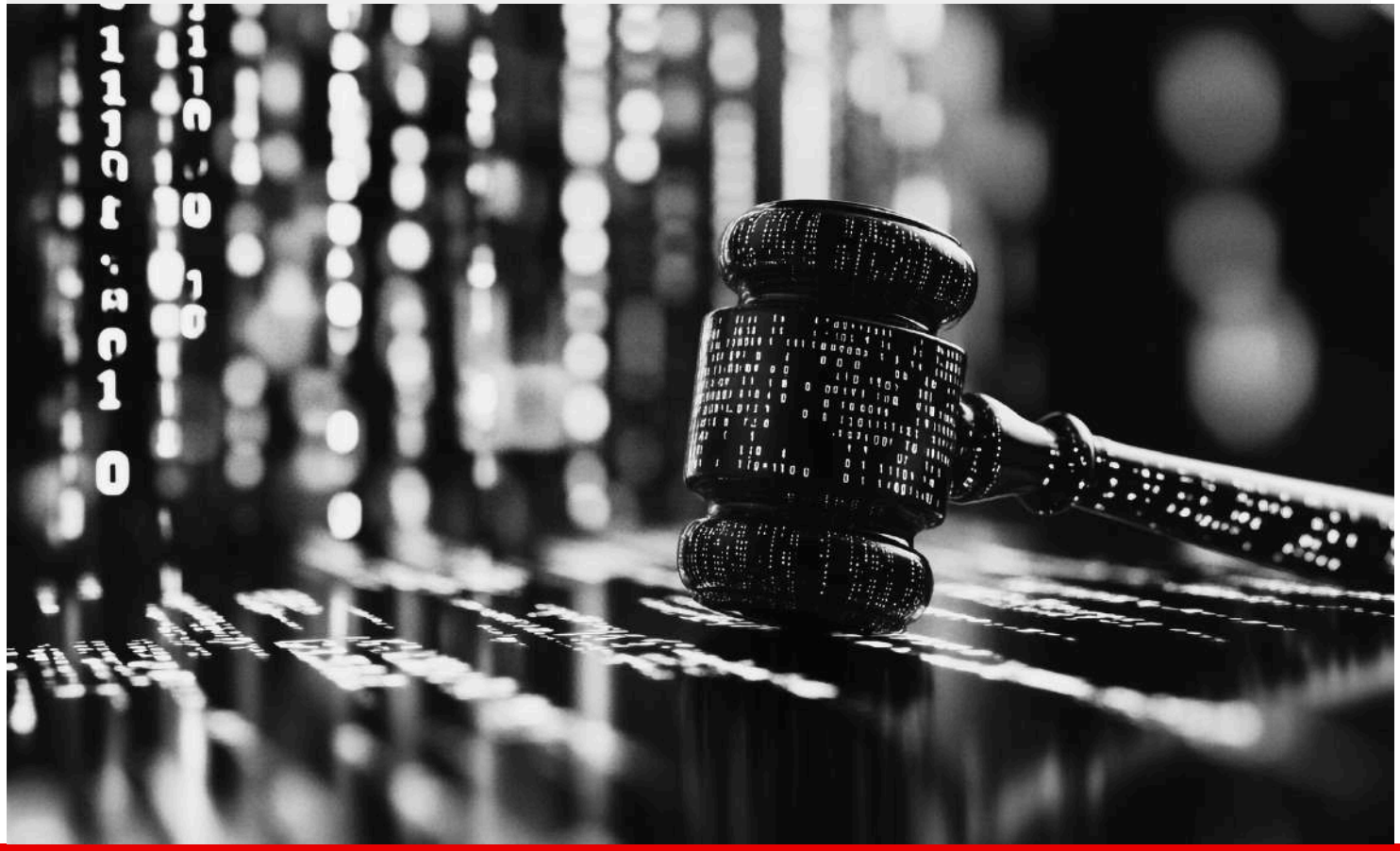
Network Rail reassured the public that the affected Wi-Fi network is a simple 'click & connect' service that does not collect personal data. Earlier this month, a similar cyberattack targeted Transport for London (TfL), raising concerns about the vulnerability of public transport systems. A teenager from Walsall, West Midlands, was arrested in connection with the TfL incident, and authorities are continuing their investigations into both the cases.

HONG KONG INTRODUCES FIRST CYBERSECURITY LAW TO SAFEGUARD ITS CRITICAL INFRASTRUCTURE

On 25 June 2024, the Hong Kong Government proposed a new cybersecurity law, the Protection of Critical Infrastructure (Computer System) Bill, to strengthen the security of critical computer systems (CCSs) that support essential services. The proposed legislation would require Critical Infrastructure Operators (CIOs) to implement specific measures to protect their systems and minimize the risk of disruptions caused by cyberattacks. The Legislative Council began consultations on the proposed law on 2 July 2024.

The Bill outlines obligations for CIOs, such as establishing strong cybersecurity management structures and responding promptly to security incidents. A new Commissioner's Office will be created to oversee the implementation of these measures. The legislation will apply only to designated CIOs and systems that are crucial to the functioning of critical infrastructure (CIs), such as energy, healthcare, financial services and transport networks.

Hong Kong's proposed cybersecurity framework aligns with similar legislation in mainland China, Singapore and Australia. Once enacted, the law is expected to improve the overall cybersecurity of Hong Kong's critical infrastructure, though concerns remain about the scope of its application and compliance requirements. The government plans to introduce the Bill in the Legislative Council by the end of 2024, with enforcement likely beginning within a year of its passage.



CYBERCRIMINALS EXPLOIT DIGITAL MARKETING TOOLS TO UNLEASH MALICIOUS CAMPAIGNS

Cybercriminals are increasingly exploiting digital marketing tools, such as Search Engine Marketing (SEM) and link shorteners, to launch sophisticated malicious campaigns. Researchers from Mandiant and Google have uncovered that these tools, traditionally used by advertisers to deliver targeted content, are now being repurposed by threat actors to evade detection and to maximize the impact of their attacks.

Cybercriminals use SEM tools to refine their malvertising strategies, identifying high-traffic keywords to lure potential victims. For example, in June 2024, keywords like "advanced IP scanner" generated over 220,000 clicks across various domains. Attackers use this data to build campaigns, mimicking legitimate ads to draw in unsuspecting users.

Link shorteners, typically used to simplify URLs, are also being weaponized. Threat actors employ them to obscure malicious URLs, often redirecting victims to phishing pages or malware downloads. Shortened links, combined with CAPTCHA technology, prevent automated security tools from detecting and analysing these threats while ensuring that human victims can still access malicious content.

Additionally, IP geolocation utilities, intended to track the geographic reach of ad campaigns, are being misused to tailor attacks based on a victim’s location. For example, ransomware like Kraken uses geolocation data to monitor infection rates, adjusting its behaviour based on the target's location to avoid detection.

While blocking these tools entirely is impractical due to their legitimate uses, experts advise organizations to focus on detection and mitigation strategies. Monitoring network telemetry for suspicious activity, analyzing link shorteners and refining CAPTCHA detection can help defend against these emerging threats. As cybercriminals continue to adapt, it is crucial for businesses to stay informed and bolster their cybersecurity measures accordingly.

ESPORTS TO MAKE DEBUT IN OLYMPICS IN 2025 AMID CYBERSECURITY CONCERNS

The International Olympic Committee (IOC) has announced that esports will officially debut in the Olympic Games, with the first Olympic Esports Games scheduled for 2025 in Saudi Arabia. This landmark inclusion of competitive gaming in Olympics reflects the immense growth of the esports industry, which has rapidly expanded in both popularity and revenue. However, as esports prepares for this milestone, report by Check Point Software Technologies highlights significant cybersecurity concerns that could threaten the integrity of future tournaments.

However there are concerns that cyberattacks targeting esports events could severely impact the industry. Common threats include Distributed Denial of Service (DDoS) attacks, which overload servers and disrupt gameplay, hacking of professional players' accounts, cheating through illicit software and data theft. These risks will jeopardise the integrity of the competition and undermine the trust of players, organizations and fans.

The esports industry faces high financial stakes, with global video game revenues projected to reach USD 455 billion by 2024. India’s gaming market alone hit USD 3.1 billion in 2023, underscoring the sector's rapid growth and appeal to cyber criminals. As the popularity of esports continues to rise, the industry increasingly becomes an attractive target for attacks, making implementing robust security measures critical.

Experts recommend that organisations in esports adopt strong cybersecurity practices to prevent disruptions. These include educating players and employees about cyber risks, securing all systems, regularly installing updates and backing up data. Implementing these preventative measures is essential for ensuring the safety and fairness of esports competitions on the stage as grand as the Olympics.

As esports is set to make its debut at the Olympics, addressing cybersecurity challenges will be vital to maintaining the sport’s credibility and protecting the interests of all stakeholders. With the right security protocols, esports can confidently enter its new role as an Olympic sport, offering a secure and competitive environment for players and fans worldwide.

COSMICBEETLE EXPLOITING OLD VULNERABILITIES TO TARGET SMBS GLOBALLY

Cybersecurity researchers at ESET, a software company specializing in cybersecurity, have revealed that cybercriminal group CosmicBeetle has been actively exploiting outdated vulnerabilities to attack small and mid-sized businesses (SMBs) worldwide. These businesses are often more vulnerable due to weaker security measures and a lack of regular security audits or incident response plans, making them attractive targets for cyberattacks.

CosmicBeetle is deploying ScRansom, a Delphi-based ransomware, leveraging known vulnerabilities such as EternalBlue (CVE-2017-0144), Zerologon (CVE-2020-1472) and others like CVE-2023-27532. ScRansom uses advanced encryption techniques, including AES-CTR-128 for file encryption, with RSA-1024 key pairs to manage keys. The malware partially encrypts files based on their extensions and renames them with the ".Encrypted" extension. It offers different encryption modes, the most severe being "ERASE," which renders files irrecoverable.

The ransomware has a graphical user interface (GUI) and includes various tools for process termination, such as ScHackTool and ScService. Using the Tox protocol, communication with victims occurs through encrypted channels, including email and qTox. Researchers noted that CosmicBeetle's decryption process is complex and often ineffective. Victims must manually run the decryptor on each infected device, inputting specific "ProtectionKeys" for corresponding "Decryption IDs," which are difficult to manage, especially when ScRansom runs multiple times on a machine, generating more IDs. In some cases, files are permanently lost, even after a ransom payment, due to the ineffective decryption or destruction by the ERASE mode.

CosmicBeetle's unsophisticated and error-prone decryption methods make recovery challenging, often resulting in incomplete data restoration. SMBs are urged to prioritize cybersecurity measures and patch outdated systems to avoid becoming easy targets for such attacks.

NCSC AND GLOBAL PARTNERS WARN OF CHINA-LINKED BOTNET CAMPAIGN TARGETING THOUSANDS OF DEVICES

The UK's National Cyber Security Centre (NCSC), in partnership with cybersecurity agencies from the United States of America, Australia, Canada and New Zealand, has issued a joint advisory warning individuals and organisations about a large-scale botnet operation linked to a China-based company. The botnet, controlled by Integrity Technology Group, has compromised over 260,000 devices (Internet-connected) globally, including routers, firewalls and Internet of Things (IoT) devices like webcams and CCTV cameras.

The advisory identifies the malicious actor group as Flax Typhoon, a group connected to the Chinese government. The advisory highlights how the compromised devices have been used for cyberattacks, such as distributing malware and launching Distributed Denial of Service (DDoS) attacks. The advisory provides technical details and mitigation strategies, urging owners to update and secure their devices to prevent them from becoming part of this botnet.

This global advisory, backed by the Five Eyes intelligence-sharing alliance, underscores the importance of securing Internet-connected devices against rising cybersecurity threats.

INDIA FACES RISING CYBERSECURITY THREATS IN SPACE AND CRITICAL INFRASTRUCTURE

As cyberattacks on satellites increase amid nation-state conflicts, India prioritises cybersecurity to safeguard its space and critical infrastructure. Shri S Somanath, Chairman, the Indian Space Research Organisation (ISRO), stressed on the need for greater cybersecurity measures, particularly for the country's space assets, that are vulnerable to attacks due to global coordination and communication systems.

India, which has nearly 60 satellites in orbit and extensive command-and-control networks, faces the same risks as other space-faring nations. During the Chandrayaan-3 moon landing, data was transmitted from various global locations, highlighting the vulnerabilities of such complex operations. Shri Somanath emphasized that satellites could easily become targets in the future.

As nation-state conflicts escalate, such as the Russian cyberattacks on Ukraine's Viasat KA-SAT network, the threat to space systems has become increasingly evident. Experts suggest that with its growing space ambitions, India could face challenges similar to those of regional rivals like China and Pakistan. With advanced cyber capabilities and a robust space programme, China may target India's ascent as a major space power.

India's rapid digitization has made it a prime target for cyberattacks, with the country experiencing more than 3,300 attacks per week per organization—which is significantly higher than the global average. In particular, the aerospace and defence sector is ranked as one of the top targets for cyber threats and ISRO reportedly faces over 100 cyberattacks daily.

Globally, other space-capable nations are also focusing on cybersecurity. The US National Institute of Standards and Technology (NIST) and MITRE Corp. have developed frameworks and tools to defend against cyber threats in space. At the same time, The Aerospace Corporation has created testbeds for real-world cyberattacks on space assets.

To address these challenges, India needs to enhance its cybersecurity capabilities. Initiatives like Atmanirbhar Bharat aim to foster homegrown technology startups and boost expertise in cybersecurity. However, a significant gap remains in the number of skilled professionals. India has more than 40,000 unfilled cybersecurity positions, and although the talent pool has grown, more training and cyber-awareness programmes are necessary to bridge this gap.

As India continues to invest in space technology and research, it must also ensure that robust security measures are in place to protect these systems. Shri Somanath highlighted that no system is completely safe, warning that India's critical infrastructure and accumulated data could be vulnerable to attacks if not adequately secured.

INDIA AND SINGAPORE STRENGTHEN TIES WITH CYBERSECURITY AND STRATEGIC PARTNERSHIPS

India and Singapore are deepening their strategic cooperation, focusing on cybersecurity, skill development, semiconductor ecosystems, and health partnerships. Prime Minister Shri Narendra Modi and his Singaporean counterpart, Mr Lawrence Wong, have agreed to enhance collaboration between the two nations' cyber emergency response teams to combat the increasing threat of cyberattacks.

Singapore's Cyber Security Agency will partner with India's National Security Council, the Ministry of Electronics and Information Technology (MeitY), and the Ministry of External Affairs to strengthen cybersecurity defences. This updated agreement builds on the 2015 Memorandum of Understanding (MOU) and will facilitate knowledge exchange on regulatory practices and training in the digital domain. A joint working group will meet regularly to ensure swift implementation of these decisions.

The nations also aim to foster digital cooperation, promoting greater interoperability between their digital economies and improving data flow and technical expertise exchanges. The partnership will extend to international forums like the UN Open-Ended Working Group on Security.

In addition to cybersecurity, a new MOU on semiconductor collaboration will help India and Singapore leverage their complementary strengths to build stronger supply chains and ecosystems. India, aspiring to become a global hub for semiconductor manufacturing, seeks to meet the growing demand for electronics and green vehicles. At the same time, Singapore aims to strengthen strategic ties with Indian manufacturers.

The countries have also agreed to cooperate on skill development, focusing on technical education, vocational training, and workforce upskilling. The MOU on health will focus on preparing medical professionals for future pandemics and improving maternal and child health. These comprehensive agreements mark a significant step towards solidifying the India-Singapore strategic partnership.

IFF HOSTS ROUNDTABLE ON STRENGTHENING AI GOVERNANCE AND REGULATION

India Future Foundation (IFF) hosted the "Data Defenders: Need for Strengthening AI Governance and Regulation" roundtable on 09th September 2024 at The LaLiT, New Delhi.
The event brought together decision-makers from the government, industry, and the academia to discuss on the importance of building a robust AI governance framework. The focus was on ethical AI development, regulatory needs and AI's role in bolstering cybersecurity. The discussions emphasized on balancing innovation with responsible AI use and creating a comprehensive AI strategy for India.

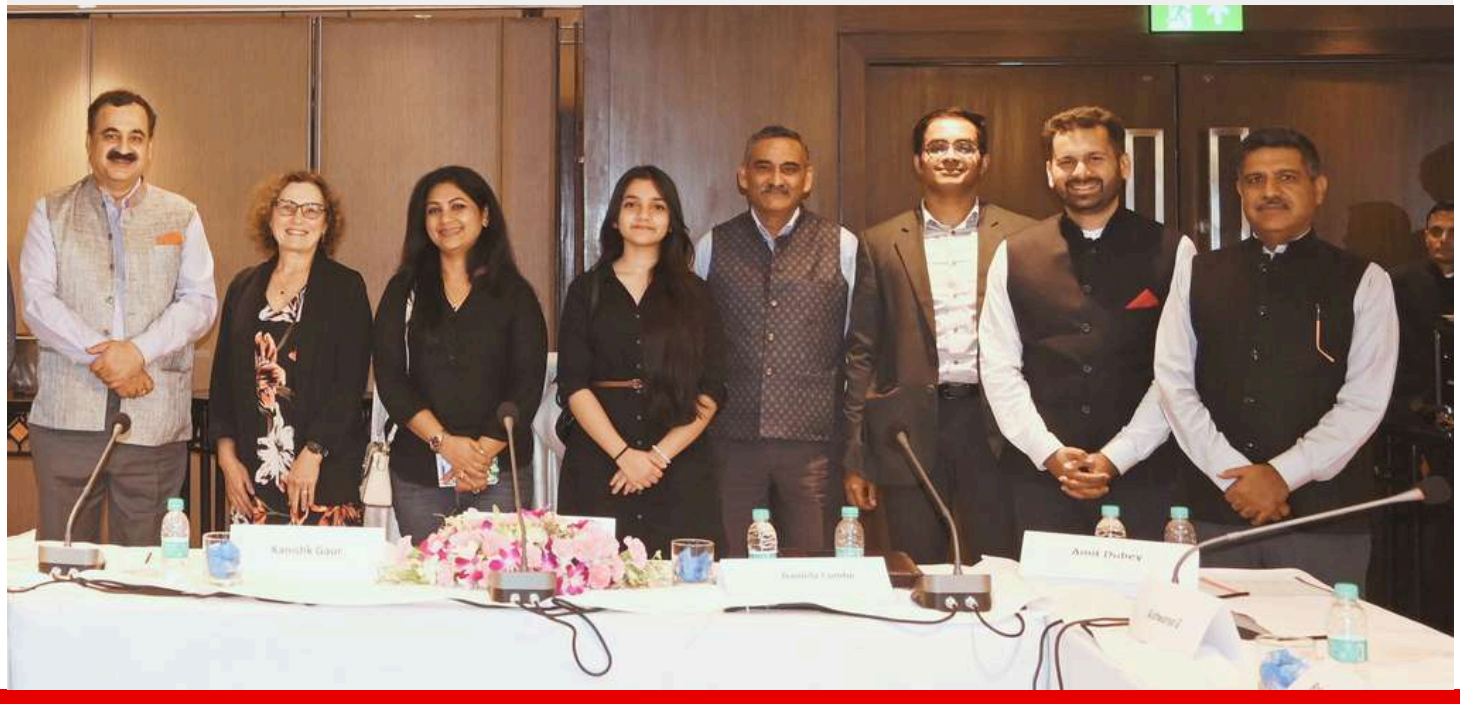
The discussions at the roundtable encapsulated the following pivotal areas:

- **Strengthening AI Governance:** Exploring regulatory frameworks, ethical guidelines and the best practices that ensure AI is governed responsibly and is aligned with India's national priorities,
- **Promoting Ethical AI Development:** Addressing the significance of ethical AI development, including the impact on national security, public trust and societal well-being.
- **Fostering Multi-Stakeholder Collaboration:** Encouraging collaborative efforts among government, industry and academia to develop comprehensive AI governance strategies that draw on diverse expertise.
- **Enhancing Cybersecurity through AI:** Exploring how AI can be leveraged to bolster cybersecurity, focusing on safeguarding critical national infrastructure and countering emerging threats.

Highlights of the Event

- **Commodore Manish Anand,** Chief Information Security Officer, Government of India, shared insights on the critical need for strengthening AI governance and its role in securing India's digital landscape.
- **Dr Pavan Duggal,** Advocate, Supreme Court of India, highlighted AI's legal challenges, emphasizing on the need for having in place well-defined regulatory frameworks to mitigate risks like privacy violations and algorithmic biases.
- **Col Kapil Jaiswal,** Director, Research (InfoSec & AI/ML), Ministry of Defence, Government of India, underscored the importance of establishing reliable AI frameworks for national security.
- **Ms Aishwarya G.**, Technology Consulting Leader, Microsoft, discussed ethical AI development, focusing on transparency, fairness and accountability in building public trust.

The discussions underscored the pressing need for India to develop a balanced regulatory framework for AI, ensuring its responsible deployment while fostering innovation. The event concluded with the participants putting forward actionable recommendations to position India as a leader in AI governance.



IFF HOSTS ROUNDTABLE ON SECURING DATA IN THE DIGITAL AGE

In collaboration with Microsoft, India Future Foundation (IFF) hosted a consultation, *"Data Defenders: Unravelling the Complexity of Securing Data"*, on 11 September 2024 at The LaLiT, New Delhi.

This event brought together experts from various sectors to discuss the challenges in data security. It explored innovative solutions to protect against the growing threats of cyberattacks, especially as a result of insider threats. The consultation featured in-depth discussions and showcased a Cyber War Game Simulation illustrating breaches caused by insider threats and their real-world impact.

The discussions at the consultation encapsulated the following pivotal areas:

- **Data Security Trends and Challenges:** Delved into the latest developments in data security, privacy regulations and emerging cyber threats, highlighting the evolving complexity of protecting sensitive information.
- **Cyber War Game Simulation:** This hands-on exercise involved participants in determining the course of action they would take in the event of a cyberattack precipitated by an insider.
- **Privacy and Compliance:** Focused on aligning organizational policies with global privacy regulations and ensuring robust compliance measures to mitigate legal and financial risks.
- **Collaborative Solutions:** The presentation stressed on the need for collaboration among stakeholders, including technology providers, regulators, and industry leaders, to foster innovative solutions for data security.
- **Strategic Incident Response:** Discussed the critical role of strategic incident response planning, including effective communication, rapid decision-making, and minimizing the long-term impact of data breaches.

Highlights of the Event

- **Mr MAKP Singh,** Former CISO, Ministry of Power, Government of India emphasised on the role of CISOs in securing organizational data infrastructure.
- **Dr Yusuf Hashmi,** Group CISO, Jubilant Bhartia Group, highlighted the dangers posed by insider threats, underscoring how insider risk remains one of the most pressing challenges in the realm of cybersecurity.
- **Mr Salil Mittal,** Cyber Security Lead, Reliance Jio Infocomm, shared insights on how insider threats affect companies holding sensitive intellectual property and the importance of having in place proactive security measures.
- **Mr Ravi Raman Tiwari,** Technical Specialist – Cybersecurity, Microsoft, stressed on the importance of proactive breach reporting under regulatory frameworks, particularly in highly regulated industries.

The consultation underscored the importance of cross-functional collaboration in managing incidents, focusing on continuous monitoring, behavioural analytics and stronger Data Loss Prevention (DLP) systems to address insider threats and data exfiltration risks.

IFF HOSTS ROUNDTABLE ON AI-POWERED TRANSFORMATION AND INNOVATION FOR PUBLIC SECTOR ENTERPRISES

India Future Foundation (IFF), in association with Microsoft, hosted the roundtable event *"Digital Horizons – AI-powered Transformation and Innovation for Public Sector Enterprises"* on 20th September 2024 at President, Mumbai - IHCL SeleQtions, Cuffe Parade.

The event aimed to explore the transformative potential of AI in revolutionising public sector enterprises by enhancing their productivity, streamlining workflows and improving service delivery through tools such as Microsoft's Copilot.

Key objectives of the event

- **Enhancing Productivity:** Demonstrating how AI solutions can automate minutes of the meeting, document verification and CRM activities, reducing manual work and increasing operational efficiency.
- **Leveraging Data and AI for Innovation:** Using Copilot's AI-driven solutions to improve productivity and thereby improve the efficiency of PSUs.
- **Supporting Sectoral Growth:** Highlight how AI can drive economic growth by fostering innovation, developing skilled talent and modernizing the PSUs.

Highlights of the Event

- **Mr Jayant Gupta,** Executive Director, Information Systems, Hindustan Petroleum Corporation Limited (HPCL), emphasized on the impact of AI-powered solutions on the public sector's ability to enhance service delivery and improve their operational efficiency.
- **Mr Nagsen Wankhede,** Chief General Manager (IT), Maharashtra State Electricity Transmission Company Limited (MSETCL), discussed how AI is helping identify patterns in reports, thereby improving audit efficiency and decision-making processes.
- **Mr Sandeep Bandivdekar,** Director - Services Partners, Microsoft, showcased Security Copilot, an AI tool that analyzes millions of logs to prevent incidents, demonstrating the potential for AI to enhance security across public sector entities proactively.
- **Mr Sumit Patni,** Director, PwC, highlighted AI's role in enriching vast public sector data, making it more accessible and localised for citizens.

The consultation underscored the importance of cross-functional collaboration in managing incidents, focusing on continuous monitoring, behavioural analytics and stronger Data Loss Prevention (DLP) systems to address insider threats and data exfiltration risks.


Copilot to talk to 3rd party System of Record (e.g. SAP)


Digital Horizons


INDIA FUTURE
FOUNDATION

IFF HOSTS ROUNDTABLE ON SAFEGUARDING DATA IN THE DIGITAL AGE

In collaboration with Microsoft, India Future Foundation (IFF) hosted *"Digital Fort Knox: Safeguarding Your Data Treasure"* on 27th September 2024 at Taj MG Road, Bengaluru.

This event brought together experts from various sectors to discuss the challenges faced, in the modern day, in the realm of data security, focusing on insider threats and cyber espionage. The session featured practical insights and strategies to help organisations protect their data in an increasingly complex digital environment, supported by a hands-on Cyber War Game Simulation to demonstrate real-world breach scenarios.

Highlights of the Event

- **Mr Ashish Sain,** Senior Vice President IT and Digital Risk Management, HDFC Bank, discussed the importance of real-time monitoring and automated incident response to mitigate data breaches.
- **Shri Nantha Ram Ramalingam,** Global Head - Cybersecurity, Dyson Technology India, highlighted the risks posed by insider threats, particularly during an employee's exit period, emphasizing on the importance of collaboration between HR, IT and CISOs.
- **Mr Amit Kumbhat,** Director of IT, Four Seasons Hotel & Private Residences, emphasized on the need for AI-driven technologies and a Zero Trust architecture to protect sensitive data.

The consultation explored strategies like improving Data Loss Prevention (DLP) systems, cross-functional collaboration, and leveraging tools for real-time monitoring and insider threat detection to secure an organisation's data effectively.

IFF IN THE MEDIA

Kanishk Gaur, Founder & CEO, IFF spoke about Rising Organized Transnational Crime on *NewsNine.*

Kanishk Gaur, Founder & CEO, IFF spoke about the Rise of Electronic Warfare and Hybrid Warfare on *India Today.*

Kanishk Gaur, Founder & CEO, IFF spoke about the Rise of Electronic Warfare and Hybrid Warfare amidst the Pager Explosions on Hezbollah on *News Nine.*

Kanishk Gaur, Founder & CEO, IFF shared his "Digital Arrest" knowledge on *India News.*

Kanishk Gaur, Founder & CEO, IFF, discussed "Balancing Free talks and being accountable" on *News Nine.*

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