INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

NEWS FROM AROUND THE WORLD

ROLE OF AI IN CYBERSECURITY

In an ever-evolving digital landscape, the relationship between Artificial Intelligence (AI) and cybersecurity has become more crucial now than it was ever before. AI, with its growing computational power and proficiency in supervised, semi-supervised and unsupervised learning, is the lynchpin of any cybersecurity measure. It plays a pivotal role in analyzing vast datasets, identifying patterns and signatures, scrutinizing user behavior, detecting anomalies and threats, automating responses and streamlining workflows for cyber compliance.

IN THIS NEWSLETTER

While the pre-COVID era witnessed the integration of AI and cybersecurity, particularly in areas like intrusion detection and non-signature-based anomalies, the post-pandemic era has seen an exponential increasing reliance on AI for safeguarding/countering cyber threats and bolstering an organisation's cyber resilience.

There are several factors which have contributed towards the growing dependence on AI. 2023 witnessed a variety of cyber-attacks, especially considering the fact that as organizations struggle to keep up with increasingly smart hackers who not inly target an organisation's computer systems but also the nation's critical infrastructure. There are various threat actors like groups who specialize in ransomware attacks, hacktivists, and insiders, who use the Dark Web.

To counter the myriad nature of challenges, use of AI is central to the strategies that Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) make to protect their organisations. Further the shortage of people, with the right talent, in the realm of cyber security also necessitates the use of AI in the said domain. AI not only lends a helping hand, in the domain of cybersecurity, it can process tons of information and most importantly learn from it.

The market for AI in cybersecurity is growing at a rapid pace. It's expected to be worth more than $60 billion worldwide by 2025, a significant increase from just over $22 billion in 2023.

BLACKBERRY'S AI CYBERSECURITY ASSISTANT

BlackBerry Limited unveiled its latest innovative offering, a Generative AI-powered assistant designed to enhance the capabilities of Security Operations Center (SOC) teams, on 16 October 2023. This enterprise-grade solution acts as a SOC Analyst, providing Generative AI-based cyber threat analysis and support to bolster the operations of Chief Information Security Officers (CISOs). It leverages private large language models (LLMs) to ensure accuracy and data privacy.

The Generative AI assistant will be available to BlackBerry's Cylance® AI customers. What sets this solution apart is its ability to predict customer needs, proactively offering information without requiring users to manually ask questions, significantly condensing research hours into mere seconds. Integrated seamlessly within the Cylance Console, it transforms the user experience into a natural workflow, eliminating the inefficiencies often associated with chatbot interactions. Cylance initially launched as the industry's pioneer AI cybersecurity solution is now being recognized as the inaugural predictive cybersecurity solution.

S[pecking about the Generative AI assistant Nathan Jenniges, BlackBerry's Senior Vice President and General Manager of Spark, the Cybersecurity Business Unit, underlined the company's dedication to innovation. He pointed out that BlackBerry had pioneered the AI cybersecurity market and reaffirmed BlackBerry's commitment to staying at the forefront of the industry.

PHILIPPINES CYBERSECURITY CRISIS

The Philippines is grappling with a cybersecurity crisis as inadequate security measures have made government websites vulnerable to cyberattacks, thereby jeopardizing sensitive data and putting millions of Filipinos at risk. A breach of the Philippine Health Insurance Corporation (PhilHealth) exemplified the state's weak security practices. An individual known as DiabloX Phantom claimed to have infiltrated and got access to significant government data, emphasizing on the urgent need for improved cybersecurity practices within the country. Historical incidents, including the "Comelec leak" in 2016, the website of the Philippine Commission on Elections (COMELEC) was defaced and personal data of 55 million Filipinos was exposed.

To ensure that such incidents do not happen in future critical areas for improvement include strengthening passwords, enhance training and implement more robust monitoring to protect sensitive data.

Previous attacks

- Hackers targeted the Philippine Health Insurance Corporation (PhilHealth) in a breach that affected millions of individuals, including overseas Filipino workers, as reported by the South China Morning Post. The breach occurred after the state insurer refused to pay a $300,000 ransom.
- Additionally, the House of Representatives website was defaced, underscoring the government's digital vulnerabilities.

The Perpetrator

A hacker named DiabloX Phantom claimed to have infiltrated five major government agencies, gaining access to significant volumes of data. He infiltrated the servers of the Philippine Statistics Authority, that is responsible for national identification cards, and the Philippine National Police's forensics database, which contains sensitive case files. He also targeted the websites of the Department of Science and Technology, the Technical Education and Skills Development Authority (Tesda), and the Clark International Airport. His tactics included exploiting weak passwords, sending malware via email, using open subdomains, and capitalizing on vulnerabilities left by other hackers.

- The "Comelec leak" in 2016 exposed personal data from up to 55 million Filipino voters. Despite the scale of this breach, no prosecutions or consequences ensued.

ISRO'S DAILY CYBER-ATTACKS

According to Sreedhara Panicker Somanath, Chairman, Indian Space Research Organisation (ISRO), the organisation is confronting a daily onslaught of more than 100 cyber-attacks. Speaking during the concluding session of the 16th edition of the c0c0n, a two-day international cyber conference organized from 4 to 7 October 2023 in Kochi, Kerala, Somanath highlighted the increased vulnerability in rocket technology due to its use of cutting-edge software and chip-based hardware. The ISRO Chairman however, made it clear that ISRO has a robust cybersecurity network to counter such attacks. The c0c0n conference, organized by the Kerala Police and Information Security Research Association, served as a platform to address cyber threats and advancements in the field. The ISRO Chairman further stated that ISRO is not only focusing on software but is also conducting tests to ensure the safety of hardware chips used in rockets. He also underlined the significance of cybersecurity in safeguarding various types of satellites used for navigation, maintenance and everyday life.

The ISRO chief recognized the dual nature of advances in technology, posing both opportunities and threats. He also stressed on the importance of research and hard work to counter cyber threats, suggesting using technology, such as artificial intelligence, to combat cybercriminals.

Kerala Revenue Minister P. Rajeev, who inaugurated the concluding session, of the c0c0n conference, commended on the state's role as a model for cybersecurity governance, noting the state government's efforts in ensuring Internet access across the state. He praised the c0c0n conference as a platform for fostering the next generation of cybersecurity experts.

The event was attended by several prominent figures, including Hibi Eden MP, Mayor M. Anilkumar, actor Mamta Mohandas, Intelligence ADGP Manoj Abraham IPS, and ISRA president Manu Zacharia.

INDIA'S DEFENCE CONCLAVE ON CYBERSECURITY

On 10 October 2023, at the India Defence Conclave, New Delhi concerns were raised about India's cybersecurity readiness, especially after the country ranked 17th out of 20 major economies in the annual MIT CyberDefense Index report. The report cited poor national digital economy adoption and weak cybersecurity regulations despite a digitally forward government and a sizeable IT-enabled service sector.

Speaking at the conclave, Lt Gen MU Nair, National Cyber Security Coordinator, highlighted the need for collaboration between the private sector, government ministries and the military to address cyber challenges. He also noted the increasing number of cyber-attacks, particularly those in the financial sector, where digital transactions and cyber-attacks have surged. Nair emphasized on the importance of cybersecurity to protect India's digital infrastructure.

At the same conclave, PS Raghavan, Chairman, National Security Advisory Board of India (NSAB), stressed on the need to strengthen India's indigenous defence industry, diversify technology acquisition and absorption and accelerate civil-military fusion. He also called for capacity building in the software sector to counter cyber threats and emphasized on the importance of ending "technology apathy" among officials.

Speaking at the same conclave, Dr Samir Kamat, Secretary, Defence Research and Development Organisation (DRDO), discussed the initiatives to promote critical and cutting-edge technologies, including the opening of 125 centers of excellence and the establishment of a Technology Development Fund.

ARGENTINA'S NEW CYBERSECURITY STRATEGY

To counter the rapidly evolving cyber threat landscape and enhance the nation's digital resilience, Argentina has approved its Second National Cybersecurity Strategy. The strategy, established via Resolution No. 44/2023, not only provides guidelines for the protection of cyberspace but also creates a new unit to oversee its implementation. The Second National Cybersecurity Strategy builds upon its predecessor, adopted in May 2019 under Resolution No. 829. The updated strategy aims to address the emerging challenges posed by the ever-accelerating pace of technological advancements.

The adoption of the new strategy follows an extensive public consultation process initiated in January 2023, which actively engaged stakeholders from the public, private and academic sectors, civil society, international organizations and the technical community. The collective input was instrumental in crafting a robust and forward-thinking cybersecurity framework.

This updated strategy defines cybersecurity as the "set of policies and actions aimed at raising the security levels of information and communication technology (ICT) infrastructures." The primary objective, of the new strategy, is to safeguard this infrastructure, which could potentially be vulnerable to various threats and security incidents. By doing so, it also aims to prevent incidents that could disrupt the functioning of the state, organizations, essential services, and ultimately, the public's welfare.

One of the pivotal components of the new strategy is the creation of the Cybersecurity Management and Cooperation Unit, which is responsible for preparing, promoting and monitoring the Strategy Action Plan. This unit will be instrumental in ensuring the effective implementation of the strategy's objectives and initiatives.

Moreover, the strategy specifies the functions of the Executive Unit of the National Cybersecurity Committee, further strengthening the country's comprehensive approach to tackling cybersecurity challenges. It underscores the importance of consolidating efforts across government bodies, the private sector, academic institutions, civil society and international partners to address the ever-evolving cybersecurity landscape collectively.

Argentina's adoption of the Second National Cybersecurity Strategy demonstrates its commitment to staying ahead of the challenges brought about by technological advancements, ensuring the protection of its critical infrastructure and fostering a more secure digital environment for its citizens and organizations. This initiative also reflects the proactive response, of Argentina, to cyber threats that are evolving which impact nations worldwide.

AVOSLOCKER RANSOMWARE UPDATE

As a part of the ongoing StopRansomware initiative that provides advisories for network defenders to protect against various ransomware variants and threat actors, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint Cybersecurity Advisory (CSA), that focuses on the AvosLocker ransomware variant. The joint advisory offers insights into recent and historical tactics, techniques, procedures (TTPs) and indicators of compromise (IOCs), of the AvosLocker ransomware variant, to help organizations bolster their defenses against ransomware.

Details of the AvosLocker ransomware variant, as mentioned in the joint advisory are largely a result of the findings based on FBI investigations carried out as recently as May 2023. AvosLocker operates under a ransomware-as-a-service (RaaS) model and has impacted organizations across critical infrastructure sectors in the United States of America. It affects Windows, Linux and VMware ESXi environments. AvosLocker affiliates gain access to organizations' networks using legitimate software and open-source remote system administration tools. Subsequently, they employ exfiltration-based data extortion tactics with threats of leaking or publishing stolen data.
This recent CSA serves as a follow-up to the one issued on 17 March 2022. Furthermore, it provides a YARA rule that the FBI developed after analyzing a tool linked to an AvosLocker compromise. The FBI and CISA strongly advise organisations in the critical infrastructure sectors to implement the mitigation recommendations outlined in this CSA to reduce their risk and impact of the AvosLocker ransomware and similar ransomware incidents.

VISA AND EXPEL ANNOUNCE PARTNERSHIP TO ENHANCE CYBERSECURITY

On 2 October 2023, Visa, a global leader in payment solutions, announced a strategic partnership with Expel, a renowned security operations provider. This collaboration marks an expansion of Visa's Value-Added Services into the emerging domain of Managed Detection and Response (MDR) for clients worldwide. Given the increasing threat of global cybercrimes, projected to cost approximately $10.5 trillion annually by 2025, this partnership aims to empower businesses of all sizes to better anticipate and safeguard against cybersecurity threats.

Speaking on this partnership, James Mirtin, Global Head of Visa's Risk and Identity Solutions, emphasized on the financial impact of cybercrimes on global businesses.

Organizations currently face many cybersecurity challenges, including the relentless expansion of the threat landscape, a continuous stream of cybersecurity alerts and events and difficulties in recruiting and retaining cybersecurity talent. Visa has taken significant measures to protect its network and is dedicated to facilitating secure global financial transactions by assisting clients in identifying and mitigating their unique cybersecurity vulnerabilities.

US RECORDS HIGH DATA COMPROMISES

In the United States of America, data breaches leading to the compromise of personally identifiable information (PII) have reached an all-time high this year, surpassing the previous record set in 2021. According to research by the Identity Theft Resource Center (ITRC), more than 2,100 organizations have reported data breach incidents in the first nine months of 2023. This surpasses the prior record of 1,862 data compromises recorded in 2021, and this year's data breaches are still ongoing, with the final three months of the year yet to be tallied.

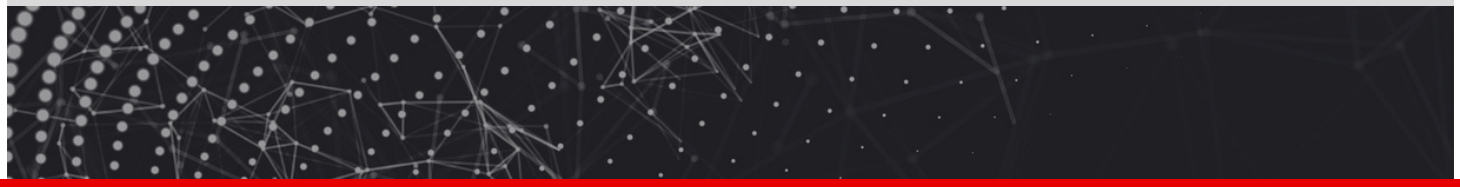
The surge in data breaches can be attributed to supply-chain attacks, with significant consequences for organizations. The ITRC report notes that most of these compromises, approximately three out of five, result from attacks against just 87 organizations. Many of these downstream victim organizations fell victim to attacks against Progress Software's MOVEit file-transfer service.

Supply-chain attacks are increasingly contributing to the growth in data breaches in 2023 and there is no indication that this trend will change, according to James Lee, Chief Operating Officer at ITRC. Vendors are attractive targets for cybercriminals due to their often limited cybersecurity resources while housing data from multiple customers. To mitigate supply-chain attacks, more robust vendor requirements and due diligence will be essential.

The report highlights that four of the top eight data compromises in Q3 2023 were related to attacks on MOVEit. Data breach notifications filed by Maximus, IBM Consulting, CareSource, and PH Tech, all linked to mass exploits of a zero-day vulnerability in MOVEit, exposed the PII of more than 20 million individuals.

The rise in zero-day attacks is closely linked to these MOVEit attacks, with ITRC reporting 86 data breach disclosures involving zero-day exploits in the first nine months of 2023, a sharp increase from the five recorded in 2022.

In total, data breaches have compromised the PII of almost 234 million individuals in the first three quarters of 2023. This number is still notably lower than the 425 million individuals impacted in 2022, primarily due to a massive breach at Twitter that accounted for more than 221 million victims, as noted by ITRC.



GOOGLE FUNDS RIT'S CYBERSECURITY PROGRAMME

Rochester Institute of Technology (RIT), New York, is set to benefit from Google's support in training students and offering cybersecurity services to local community organizations. RIT is already actively engaged in cybersecurity research and offers degree programmes. Now, it will receive $500,000 in funding from Google for a cybersecurity clinics initiative. Google's philanthropic organization, Google.org, is leading the initiative.

ACCENTURE ACQUIRES MNEMO MEXICO

Accenture has acquired MNEMO Mexico, a managed cybersecurity services company based in Mexico City. MNEMO Mexico, founded in 2012, boasts of a team of 229 cybersecurity professionals holding 180 cybersecurity industry certifications. Their services include advanced cyber defence and response capabilities, a cyber intelligence platform powered by generative AI and other advanced technologies, and a 24*7 security operations centre in Mexico City. The company serves clients across various industries, including telecommunications, banking and insurance.

By adding MNEMO Mexico to its portfolio, Accenture strengthens its cybersecurity capabilities and extends its local resources in Mexico and Latin America. This move comes in response to the increasing demand for managed security services in the region. Mexico consistently ranks among the Latin American countries most affected by cyberattacks and a joint report with the World Economic Forum's Global Cybersecurity Outlook revealed that talent recruitment and retention is a crucial challenge for managing cyber resilience, with less than half of respondents reporting having the necessary skills to respond to cyberattacks.

The acquisition aligns with Accenture's efforts to enhance its cybersecurity services and expand its presence in Latin America.

INDIAN PM'S CALL FOR CYBERSECURITY

Indian Prime Minister Narendra Modi has emphasized on the importance of India achieving self-reliance in cybersecurity, encompassing hardware and software. He stressed that having control over the entire value chain is crucial to ensuring the security of the country's digital infrastructure.
At the seventh edition of the India Mobile Congress that was held in New Delhi, the Indian Prime Minister had called for self-reliance in cyber security, in the entire manufacturing value chain. This call for self-reliance holds significance, mainly as India has previously considered imposing restrictions on the import of laptops and computers, mainly due to concerns about the security of digital networks, given that many of these imports originate from China.
Furthermore, the Prime Minister urged India to position itself as a thought leader in technology. He suggested that India should transition from being an adopter and implementer of technology to becoming a thought leader in the said field.

DATA SECURITY CONCERNS IN INDIA

In an era marked by rapid digital transformation and development of advanced technologies, India faces growing concerns about the security of its massive data reservoirs. The country's proximity to adversaries and the increasing sophistication of cybercriminals necessitates a collaborative effort among Indian technologists and business executives to build a robust cybersecurity ecosystem. Experts highlighted these challenges during Singapore Cyber Week 2023, held from October 17 to 19.

Over the past six months, several industries in India, including Healthcare, Education/Research and Utilities, have witnessed a surge in cyberattacks. On an average, each Indian organization faced 2,157 weekly attacks, compared to the global average of 1,139 attacks per organization, according to Check Point's Threat Intelligence Report.

Cybersecurity has become increasingly complex, with evolving threats and sophisticated attacks that can be challenging to understand and combat.

The accelerated digital transformation of healthcare institutions, in particular, during the COVID-19 pandemic, led to a zero-touch approach to healthcare services. However, this digitalization often lacked a security-first perspective, resulting in security gaps and vulnerabilities.

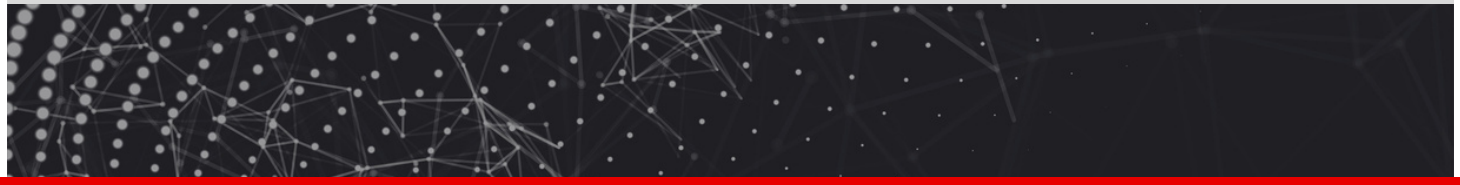
Despite these challenges, India's technological landscape is advancing, with venture capital investments in the country's digital ecosystem and a growing pool of talented individuals returning home after studying abroad. India is also building data centers to store sensitive information within its borders.

However, experts warn against complacency and stress the need for continuous vigilance and collaboration to address evolving cyber threats effectively.

CERT-IN WARNS OF VULNERABILITIES

Google Chrome desktop users have been alerted to a high-risk hacking threat by the Indian Computer Emergency Response Team (CERT-In), the national nodal agency for responding to computer security incidents as and when they occur, has issued a warning about vulnerabilities in older versions of the web browser that could potentially allow remote hackers to access systems and execute malicious operations.

CERT-In, a nodal agency under the Ministry of Electronics and Information Technology, labelled this threat as high-severity in its advisory. They identified multiple vulnerabilities in the desktop version of Google Chrome, which remote attackers could exploit to bypass security restrictions, execute arbitrary code, or cause denial of service conditions on the targeted system.



NEWS FROM AROUND THE WORLD

The affected versions of Google Chrome are those before 117.0.5938.132 version on Windows, Mac, and Linux platforms. The vulnerabilities include a heap buffer overflow in vp8 encoding in libvpx and a use-after-free error in Passwords and Extensions. Remote attackers could exploit these vulnerabilities by using a specially crafted HTML page, potentially redirecting users to malicious websites and gaining unauthorized access to systems. Once inside, attackers could execute arbitrary code and launch a denial of service attack, rendering the system unusable for legitimate users.

CERT-In advises users to update their Google Chrome desktop browser to the latest stable channel version to mitigate these vulnerabilities.

THEME OF THE MONTH

PROTECTING OUR DIGITAL FRONTIER - CYBERSECURITY AWARENESS MONTH

Cybersecurity Month in October reminds us of the ever-growing importance of safeguarding our digital lives. By raising awareness, promoting best practices, and fostering collaboration, we can collectively work towards creating a more secure digital environment. Implementing fundamental cybersecurity principles is essential for individuals and organizations in this inter-connected world. Together, we can build a more robust digital fortress and protect our valuable data and personal information from the ever-evolving threat landscape.

The Significance of Cybersecurity Month

Cybersecurity Month was established to serve several crucial purposes:

Raise Awareness: In the digital age, where our personal and professional lives are closely intertwined with technology, it's imperative to understand the potential risks. Cybersecurity Month aims to educate individuals about the various cyber threats, from phishing to ransomware attacks and the consequences they can have on our lives.

Promote Best Practices: Cybersecurity is a shared responsibility. By highlighting best practices, individuals and organizations can improve their digital defence mechanisms, reducing the likelihood of breaches and data theft. This includes everything from regularly updating software to using strong, unique passwords.

Encourage Collaboration: Governments, businesses, and individuals must work together to combat cyber threats effectively. Cybersecurity Month fosters stakeholder collaboration, including governments, law enforcement agencies, and cybersecurity experts. Sharing information and insights is vital to creating a safer digital environment.

THEME OF THE MONTH

Empower Individuals: Everyone, from children to senior citizens, must have a basic understanding of cybersecurity. Cybersecurity Month empowers individuals with the knowledge and tools needed to protect themselves online, enabling them to navigate the digital world with confidence.
Key Cybersecurity Principles

Strong Passwords: A robust and unique password is the first defense against cyberattacks. Make use of a combination of letters, numbers, and symbols. Consider using a password manager to generate and store complex passwords for different accounts.

Regular Updates: Keep all your software, operating systems, and applications current. Cybercriminals often exploit vulnerabilities in outdated software, so updating is essential.

Be Cautious of Phishing: Be vigilant against phishing emails and messages. Cybercriminals often impersonate reputable organizations to trick individuals into revealing personal information or clicking on malicious links.

Use Two-Factor Authentication (2FA): Enable 2FA wherever possible. This provides an additional layer of security by requiring you to enter a code sent to your mobile device or email when logging into an account.

Protect Personal Information: Avoid oversharing personal information on social media and other online platforms. The more cybercriminals know about you, the easier for them to craft convincing attacks.

Regular Backups: Back up your data regularly to ensure you can recover it in case of a cyberattack. Use offline or cloud-based solutions to keep your data safe.

Educate and Train: Organizations should provide cybersecurity training for employees to ensure they understand the risks and best practices. Likewise, parents and educators should educate children about online safety.

CLOUD & E-GOVERNANCE PROGRAMME

In a significant move, the India Future Foundation (IFF) partnered with Uttar Pradesh Development Systems Corporation Ltd (UPDESCO) and Amazon Web Services (AWS) to host a one-day programme, "Cloud for Digital Transformation and E-governance." The event brought together government officials in the erstwhile city of Nawabs on 11 October 2023.

The event marked an exciting step towards the digital future of Uttar Pradesh. Government officials, along with tech enthusiasts, gathered to explore the potential of cloud computing for modernizing governance in the state.

The event featured esteemed speakers from the government sector. Neha Jain, IAS, Managing Director, of UPDESCO and Special Secretary for Information Technology, Government of Uttar Pradesh, set the stage with her enlightening keynote address, stressing on the role of technology in the state's progress. Mohit Agarwal (IPS), Additional Director General of Police- Anti-Terrorist Squad, Uttar Pradesh, provide his insights, emphasizing on the importance of digital transformation.

Their presence underscored the state's ambitious goal of becoming self-reliant and reaching a remarkable $1 trillion economy.

But this event wasn't just about the speakers; it was a collective effort. Bhanupreet Saini, Vijaya Sakunala, and Aloke Baidya, from AWS, shared their expertise on cloud migration and technology integration, making complex concepts easy to understand. They showcased how technology could help the state's economy gallop further.

IFF also expressed profound gratitude to those behind the scenes who worked tirelessly to make the event successful. Kanishk Gaur, Pankaj Anup Toppo, Rakesh Maheshwari, Manmeet Randhawa, Amit Dubey and Nikhil Bansal provided invaluable support and guidance, ensuring everything ran smoothly.

This one-day programme wasn't just a gathering of experts; it was a platform for collaboration, knowledge-sharing, and visionary thinking. Government officials, tech experts and dynamic leaders painted a bright future of Uttar Pradesh's journey into the digital age.

IFF IN THE MEDIA

Kanishk Gaur, CEO, India Future Foundation, shares his views on the urgent need for stringent enforcement actions against news age threats like cyber bullying on NEWS18

Kanishk Gaur, CEO, India Future Foundation gives his insights in to Paytm scams on New Nine.

Kanishk Gaur, CEO, India Future Foundation, shares his views on the AppleSnoopRow on Republic TV

Kanishk Gaur, CEO, India Future Foundation, shares his insights on the AppleSnoopRow on India Today TV

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