INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

IN THE SPOTLIGHT

CROWDSTRIKE OUTAGE CAUSES GLOBAL DISRUPTION

On July 19, 2024, a significant IT outage caused by a software update from cybersecurity firm CrowdStrike disrupted businesses and institutions across multiple countries. The outage, affected machines running the Microsoft Windows operating system (version), led to widespread chaos in transportation, banking, media and government services.

CrowdStrike reported that the issue stemmed from a defect in its Falcon sensor product, resulting in what is known as the “blue screen of death” error. This problem locked users out of their systems. Infact George Kurtz, CEO of CrowdStrike, confirmed that the outage was not due to a cyber incident and apologised for the disruption, assuring that a fix had been deployed. Authorities, including France’s cybersecurity agency ANSSI and Australia's National Cyber Security Coordinator, confirmed that there was no evidence of a cyberattack, attributing the issue to a technical defect in the software update.

IN THIS NEWSLETTER

The outage had significant global repercussions:

- **Transportation:** Major airlines such as Delta Air Lines, United Airlines and American Airlines in the U.S. were grounded. Airports worldwide, including those in Australia, the UK, Germany, India, Malaysia, the Philippines and Spain, witnessed flight delays and operational disruptions.

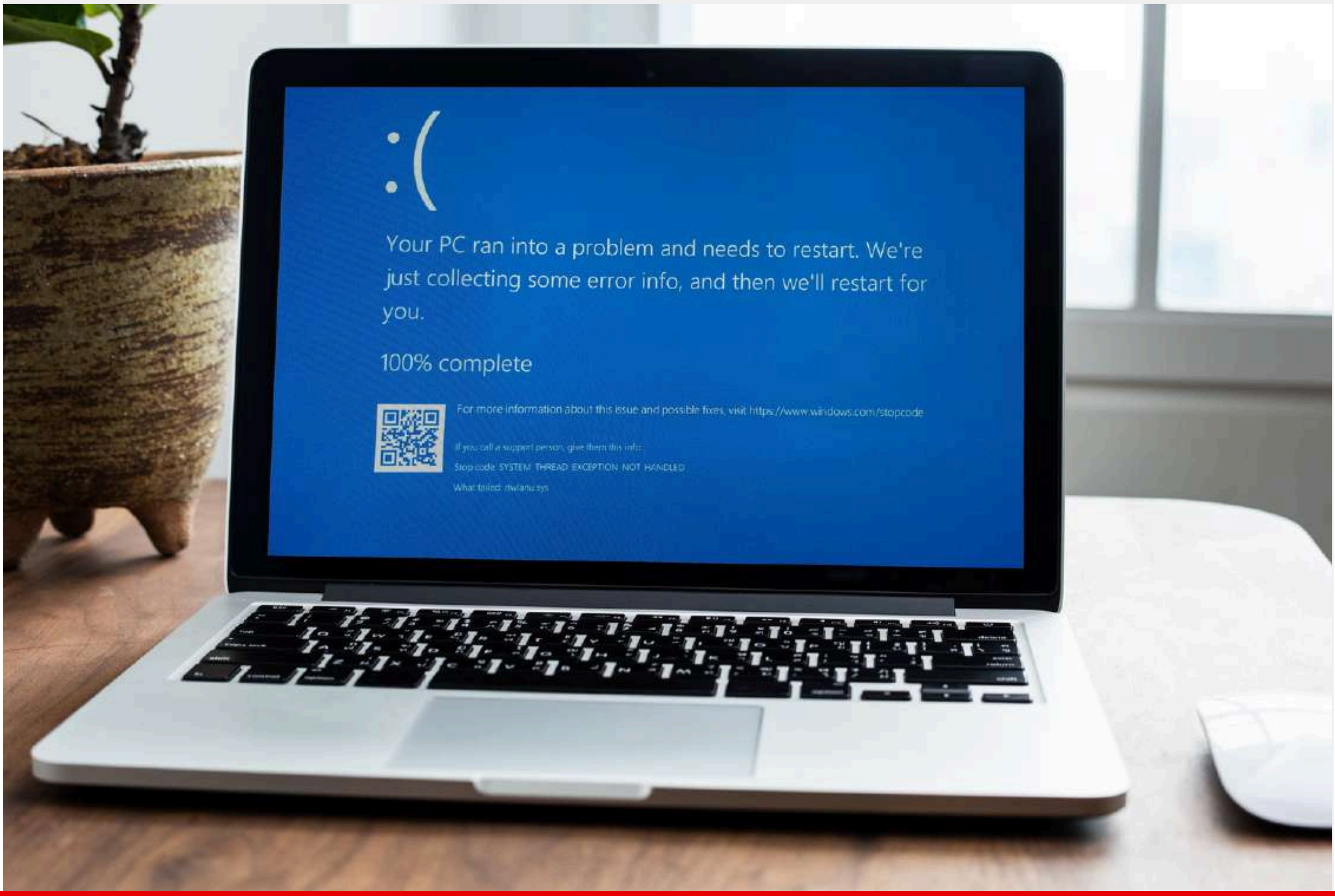
- **Banking and Financial Services:** Institutions in Australia, India, and South Africa reported service disruptions. The London Stock Exchange faced a technical glitch affecting its news service.

- **Media:** News broadcasts too were severely disrupted. Australia’s national broadcaster, ABC and Network Ten, and the UK's Sky News experienced significant outages.

- **Government Services:** Systems used by UK doctors and services of the UAE's Ministry of Foreign Affairs were impacted. Emergency services in Victoria (Australia) and New Zealand's parliamentary computer systems were also affected.

- **Other Sectors:** Supermarkets, telecom sector and health systems faced significant challenges due to the outage.

Despite the extensive impact, some services began to return to normal. Major U.S. banks and stock exchanges reported minimal disruptions and systems at Sky News and South African lenders Capitec Bank and Absa were restored.



:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

100% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:

Stop code: SYSTEM THREAD EXCEPTION NOT HANDLED

What failed: nwlanu.sys

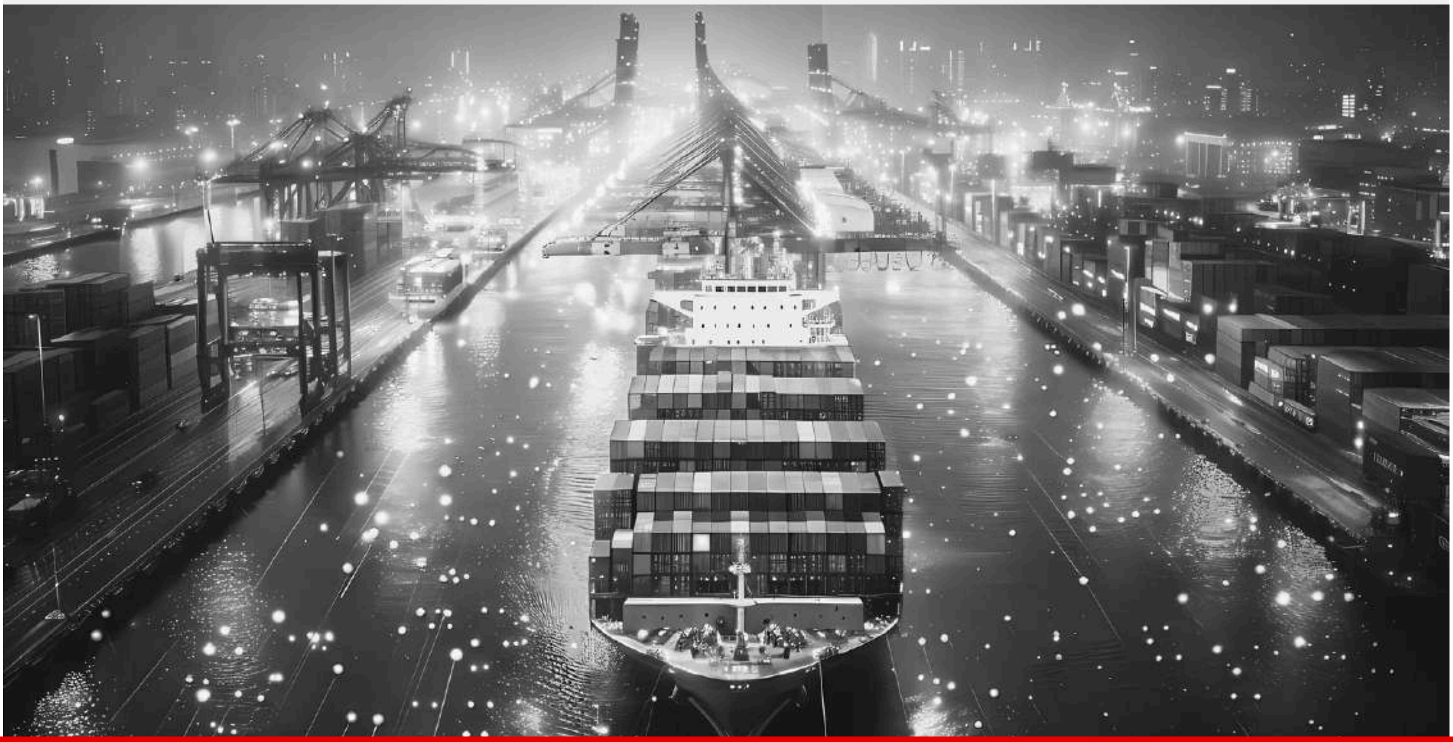
CYBER ATTACKS ON THE SHIPPING INDUSTRY RISE

The shipping industry is, in the present times, facing a pressing issue—a significant surge in cyberattacks. This alarming trend, fuelled by geopolitical tensions have prompted state-linked hackers to target trade flows, demanding immediate attention. A research by researchers from the NHL Stenden University of Applied Sciences, in the Netherlands, has revealed that shipowners, ports and other maritime groups have encountered at least 64 cyber incidents in 2023. This marks a sharp increase from three incidents a decade earlier and none in 2003.

Data from the University, which specialises in training mariners, reveals that over 80 per cent of identified incidents, since 2001, with a known attacker originated from Russia, China, North Korea, or Iran. According to Guy Platten, Secretary-General of the International Chamber of Shipping, which represents shipowners controlling about 80 per cent of the world's commercial fleet, the rise in cyber threats has placed the international rules-based order, beneficial to the shipping industry since the Second World War, under unprecedented strain.

Recent state-linked attacks have highlighted the destabilising effect of global conflicts, from Ukraine to the Middle East, on international trade. These conflicts disrupt the shipping industry, which delivers over 80 per cent of internationally traded goods, across the globe. The sector, which has historically faced physical security threats, is now grappling with its unpreparedness, especially with regards to the new challenges, in the digital space.

Dr Stephen McCombie, a maritime IT security professor at NHL Stenden University, pointed out that IT spending in the marine sector is low. Shipowners are in search of individuals with both maritime and cybersecurity expertise, but this is a small and specialised group. Experts warn that cyber-attacks could exacerbate the chaos for shipowners, who are already dealing with the impact of global conflicts' on trade routes.



The increasing digitisation of ships and Internet-enabled devices, facilitated by low-earth orbit satellites, is opening up new avenues for cyberattacks. Shri Tom Walters, a shipping lawyer at HFW, who has assisted clients with such incidents, cautioned that a cyberattack on a ship's systems could lead to disruptions similar to the Baltimore bridge crash earlier this year. This incident, which cause the closure of one of the US's busiest ports and forced carmakers to reroute shipments, is a stark reminder of the potential chaos cyberattacks can cause, especially when it comes to disrupting global shipping routes.

Noteworthy cyber incidents include a 2020 attack on Iran's Rajaee Port, which handles nearly half of the country's foreign trade, and an attack last year that took down the Port of Rotterdam, Europe's largest port. In 2017, AP Møller-Maersk, an integrated container logistics company operating in 130 countries, which controls about 15 per cent of the world's container shipping capacity, was unable to take orders from customers and had to reroute ships after its IT systems were taken offline by the NotPetya malware attack, which was attributed to Russian agents.

Dr McCombie added that cybercriminals increasingly see opportunities to extort money, understanding that these industries need to keep operating and are more likely to pay the ransom to restore their systems.

BLINKEN AND ALLIES WORK TOWARDS MARITIME SAFETY

On 29 July 2024, top diplomats from Japan, the United States of America, Australia and India met in Tokyo, Japan, to develop measures to reinforce maritime safety and cybersecurity in the Asia-Pacific region. This meeting, which was part of the Quad talks, focused on supporting other Asia-Pacific countries in enhancing their defences amid growing regional tensions.

Japanese Foreign Minister Yoko Kamikawa, US Secretary of State Antony Blinken, Australian Foreign Minister Penny Wong, and India’s External Affairs Minister Shri Subrahmanyam Jaishankar expressed severe concerns about regional tensions and strong opposition to unilateral changes to the status quo through coercion. They highlighted the militarisation of disputed features and coercive manoeuvres in the South China Sea as a major concern without directly naming China in their joint statement.

Several regional governments contest China's extensive territorial claims over the South China Sea, a crucial area for maritime trade routes and potential energy reserves. China also claims Taiwan as its territory, with the intention of annexing it by force if necessary.

During the Quad talks, the four Foreign Ministers agreed on several initiatives to counter cyberattacks, ensure maritime security and combat misinformation. They announced expanded support for Southeast Asian countries and Pacific islands to enhance their capabilities in these areas, aiming to extend the Quad's partnerships.

One key initiative involves launching a maritime legal dialogue focusing on the international law for the sea. The ministers committed to contributing to a free and open maritime order that is consistent with the U.N. Convention on the Law of the Sea in the Indian and Pacific Ocean. They pledged to enhance cooperation and coordination in these regions.

Additional support includes installing a secure telecommunications network in Palau, in the Pacific Ocean, and building cybersecurity capacity in the Philippines and India. The ministers reaffirmed their commitment to improving regional connectivity by developing resilient infrastructure such as undersea cables.

The talks followed the "2+2" security meeting between Japan and the United States, during which they identified China as "the greatest strategic challenge." Both countries agreed to deepen military cooperation, upgrade command structures, and bolster Japanese production and repair of U.S.-licensed weapons.

AUSTRALIA APPOINTS NEW MINISTER FOR CYBERSECURITY

On 28 July 2024, Australia’s Prime Minister, Anthony Albanese announced a cabinet change, appointing Tony Burke as the new Minister for Home Affairs and Cybersecurity. Tony Burke will also handle responsibilities for Immigration, Multicultural Affairs and Arts and serve as the Leader of the House.

This appointment comes two years after Clare O’Neil took on the role of cybersecurity minister when cybersecurity became a standalone portfolio. During O’Neil’s tenure, Australia experienced numerous cyberattacks and data breaches, including four of the largest in the country’s history—Optus, Medibank, Latitude and MediSecure.

Additionally, Prime Minister Albanese named Andrew Charlton as the Special Envoy for Cyber Security and Digital Resilience. Prime Minister Albanese emphasised on the importance of this role in addressing the challenges and opportunities presented by technological advancements, ensuring that Australia positions itself to avoid negative consequences while seizing positive opportunities.

INDONESIA STRENGTHENS CYBERSECURITY AFTER RANSOMWARE ATTACK

On 13 July 2024, a significant ransomware attack in Indonesia severely disrupted its national data system, prompting an urgent evaluation of its digital technology policies and its commitment to strengthening cyber resilience. Indonesian Coordinating Minister for Political, Legal and Security Affairs, Hadi Tjahjanto announced the government's plans to enhance digital security and fortify the national data centre's system capabilities. The improvements include multiple layered backups to create an unhackable system thereby ensuring that the government can effectively and in a unhindered manner serve the public.

The Ministry of Communication and Informatics is set to implement a "tenant redeploy" programme from August to September 2024, that is aimed at improving digital security governance with stricter standard operating procedures. The ransomware attack, which began on 17 June 2024, lasted for almost a week and in the process disrupted the functioning of 282 institutions, including immigration services and educational institutions, during the student enrollment period. The attacker, behind these attacks initially demanded an $8 million ransom.

Following the incident, there has been a public outcry for the Communication and Informatics Minister's resignation due to the failure to protect public data. The financial sector in Indonesia, recognising its vulnerability, is enhancing its cybersecurity capacity through standards compliance and simulations.

Indonesia's Financial Services Authority introduced cybersecurity guidelines for financial sector technology innovation, focusing on data protection, risk management, incident response and collaborative information exchange. Meanwhile, the Indonesian Internet Service Providers Association (APJII) is forming a cybersecurity task force to prevent adverse impacts from technological innovations.

RANSOMWARE ATTACK
Your personal files are encrypted
You have 5 days to submit the payment!!!
To retrieve the Private key you need to pay
Your files will be lost

HACKERS LEAK 10 BILLION PASSWORDS IN MAJOR BREACH

On 4 July 2024, a massive data breach saw the leakage of approximately 10 billion passwords on an online hacking forum. The compilation file, containing old and new password breaches, poses a considerable threat, primarily through credential stuffing attacks. This method involves hackers using a single breached password to access multiple accounts belonging to the same user.

An International Monetary Fund (IMF) report highlighted the escalating threat landscape, noting that malicious cyberattacks have doubled globally since 2020. The financial sector has been particularly hard hit, with 20,000 attack attempts, alongside significant impacts on the healthcare sector. Notable credential-stuffing attacks have already compromised users across major platforms like AT&T, Santander Bank, Ticketmaster, and 23andMe.

Despite the alarming scale of the breach, some analysts suggest that the sheer size of the leaked file might render it less usable for hackers. Nonetheless, this incident underscores the critical vulnerabilities in online security systems that need urgent addressing.

SINGAPORE LAUNCHES CYBERSECURITY SKILLS PATHWAY

The Singapore Computer Society (SCS) has unveiled a new skills pathway to bridge the talent gap in response to the growing global shortage of cybersecurity professionals. Education Minister, Chan Chun Sing announced the initiative during the SkillsFuture Festival Opening Forum on 11 July 2024.

The newly launched Skills Pathway for Cybersecurity is designed to provide clear guidelines on the skills and certifications required for careers in cybersecurity. It offers individuals opportunities to gain practical experience through internships and job interviews. Supported by 13 prominent employers, including ST Engineering and Temasek, the pathway will help individuals demonstrate their capabilities and secure opportunities in the cybersecurity field.

Chan Chun Sing highlighted the pathway's dual benefit. It assists individuals in identifying and acquiring necessary skills and certifications while helping employers recognise competencies gained through various forms of learning. This initiative aims to connect talent with industry needs more effectively.

The move comes as the global demand for cybersecurity professionals reaches critical levels. According to the World Economic Forum, there is a need for nearly four million cybersecurity experts worldwide, with the market expected to soar to more than 85 million by 2030.

The new pathway reflects Singapore’s commitment to addressing the cybersecurity talent shortage and supporting the development of a skilled workforce in the Asia-Pacific region.

MODI URGES CYBERSECURITY MEASURES FOR BUREAUCRATS

On 17 July 2024, Prime Minister, Narendra Modi highlighted a critical cybersecurity practice during a meeting with senior bureaucrats. He emphasised on the importance of logging out of IT systems at the end of each workday as a simple yet crucial measure to safeguard sensitive information from getting leaked in cyberattacks.

PM Modi shared his practice of logging out at the end of the day and recommended that offices assign someone responsible for ensuring that all systems are logged out, at the end of the day. This practice aims to reduce vulnerabilities to cyberattacks.

In addition, PM Modi referenced his recent discussion with Bill Gates about the global importance of cybersecurity and the need for vigilance against evolving threats.

Following the meeting, the Cabinet Secretary, Rajiv Gauba, issued directives to all ministries, stressing the need for robust cybersecurity practices and adherence to guidelines.

The Government of India has also significantly increased funding for cybersecurity initiatives. The budget for the Indian Cybercrime Coordination Centre (I4C) has gone up by 70 per cent, and the overall cyber coordination budget has increased by 900 per cent compared to 2022. This boost reflects the Government of India’s commitment to enhancing cybersecurity infrastructure.

AGENCIES WARN OF CHINA-LINKED APT40 EXPLOIT ADAPTATION

Cybersecurity agencies from Australia, Canada, Germany, Japan, New Zealand, South Korea, the U.K., and the U.S. have issued a joint advisory about the cyber espionage group APT40, linked to China. The group is noted for quickly adapting to newly disclosed security vulnerabilities into effective exploits within hours or days of public release.

APT40 is been known by many names like Bronze Mohawk, Gingham Typhoon and MUDCARP, Periscope, Temp.Periscope and Temp.Jumper. The group is suspected to be based in Haikou, China, and has targeted various organisations globally, including those in Australia and the U.S.

In July 2021, the U.S. and its allies attributed APT40 to China's Ministry of State Security (MSS) and indicted several members for orchestrating extensive campaigns to steal trade secrets and intellectual property.

APT40's recent activities include exploiting vulnerabilities in WinRAR (CVE-2023-38831) and public software like Log4j, Atlassian Confluence, and Microsoft Exchange. The group has also used reconnaissance frameworks and phishing campaigns, such as the ScanBox and BOXRAT backdoor, to infiltrate networks.

Notably, APT40 has been involved in recent compromises of significant institutions, including the New Zealand Parliamentary Counsel Office, in 2021. The group frequently employs web shells to maintain persistence and uses out-of-date or unpatched devices to evade detection.

Mandiant reports that APT40’s tactics include leveraging network edge devices and operational relay box networks to enhance stealth and avoid detection. Attack chains often involve reconnaissance, privilege escalation and lateral movement using the remote desktop protocol (RDP) to steal credentials and exfiltrate information.

To mitigate risks from such threats, organisations should implement robust logging mechanisms, enforce multi-factor authentication (MFA), maintain a comprehensive patch management system, replace outdated equipment, turn off unused services and ports and segment networks to protect sensitive data.

OFFENSIVE AI: THE SINE QUA NON OF CYBERSECURITY

In the ongoing evolution of cybersecurity, Offensive AI has emerged as a critical tool for understanding and countering sophisticated cyber threats. The journey from the first computer virus, Creeper, to the latest advancements in AI-driven malware underscores the need for advanced defensive strategies.

The Creeper virus, developed in 1971, marked the inception of computer viruses and highlighted the need for antivirus solutions like Reaper, which was created to combat the Creeper. This early instance of cyber conflict set the stage for the evolution of cybersecurity practices.

As cyber threats became more complex, so did the defensive measures. Today, digital security involves a range of technologies, such as firewalls, load balancers and Intrusion Detection and Prevention Systems (IDPS). Despite these advancements, the emergence of offensive AI represents a new frontier in cybersecurity challenges.

In 2023, Foster Nethercott's whitepaper at SANS Technology Institute revealed how threat actors could exploit generative AI tools like ChatGPT to create sophisticated malware that bypass traditional security controls. This insight, along with other research on advanced worms and polymorphic malware, illustrates the growing sophistication of cyber threats.

The need to develop and understand Offensive AI has become crucial. Cybersecurity professionals can better prepare and defend against these advanced threats by studying and simulating them. This approach aligns with Plato's adage that "Necessity is the mother of invention," reflecting the ongoing arms race between attackers and defenders in the cyber realm.

Professionals are encouraged to attend workshops such as the upcoming "Offensive AI for Social Engineering and Deep Fake Development" at SANS Network Security 2024 to explore Offensive AI further. This event will offer practical insights and hands-on experience with Offensive AI tools and techniques, preparing attendees for the evolving landscape of cybersecurity threats.

INDIA ENHANCES CYBERSECURITY AMID INTERNET GROWTH

According to TRAI, India has emerged as a global leader in the digital landscape, boasting 936 million Internet subscribers as of December 2023. This significant online presence has integrated the Internet into daily activities such as business transactions, education, financial activities and accessing government services, earning Indians the moniker 'Digital Nagriks.'

Recognising the critical importance of a secure digital environment, the Government of India has implemented robust policies to safeguard its vast online community. These measures aim to ensure a safe, trusted, and secure cyberspace amidst the growing prevalence of cyber threats and attacks.

The Indian Computer Emergency Response Team (CERT-In), established under Section 70B of the Information Technology Act, 2000, is crucial in this endeavour. Operating a 24x7 incident response Help Desk, CERT-In provides comprehensive incident prevention and response services and security quality management to enhance cybersecurity nationwide. CERT-In collaborates with service providers, regulators and law enforcement agencies (LEAs) to track and turn off phishing websites and investigate fraudulent activities. It also issues advisories to ministries and the RBI to strengthen cybersecurity measures and operates as an automated cyber threat exchange platform for sharing alerts across sectors.

CERT-In manages the Cyber Swachhta Kendra to detect and remove malicious programmes and conduct cybersecurity mock drills and training workshops. Additionally, the Indian CyberCrime Coordination Centre (I4C) and the National Cyber Crime Reporting Portal enable coordinated responses to cybercrimes and provide a platform for public reporting.

The Government of India has also launched the Citizen Financial Cyber Fraud Reporting and Management System, which includes a toll-free helpline (1930) to facilitate the immediate reporting of financial frauds and prevent fraudsters from siphoning funds.

In parallel, the Digital Personal Data Protection Act, 2023 upholds the individuals' rights to safeguard their data. This Act enforces data protection principles, including consent for lawful use, limiting data collection, ensuring data accuracy, and implementing robust security measures. It also imposes stringent protection on personal data transfers, such as the RBI's directive mandating the storage of payment system data within India.

As India continues its digital transformation, maintaining stringent data protection standards and robust cybersecurity measures will foster trust, resilience, and sustainable growth in its digital economy.

BUDGET 2024 INCREASES CYBERSECURITY AND AI FUNDING

The Union Budget 2024-25, presented by Finance Minister, Nirmala Sitharaman on 23 July 2024, has significantly increased funding for cybersecurity and AI projects, totalling Rs 1,550 crore. This marks a jump of over 84 per cent compared to the previous year.

Key allocations include:

- **Cybersecurity Projects:** Rs 759 crore, nearly 90 per cent more than the last fiscal year.
- **CERT-In:** Rs 238 crore for the Indian Computer Emergency Response Team (CERT-In).
- **Cybercrime Prevention:** Rs 52.8 crore for schemes addressing cybercrimes against women and children.
- **Data Protection Board:** Rs 2 crore for the newly established board under the Digital Personal Data Protection Act, 2023.
- **IndiaAI Mission:** Rs 551 crore to strengthen AI research and development.
- **IIT Kharagpur's AI Centre of Excellence:** Rs 255 crore for AI and machine learning research.

The increased budget reflects India's commitment to enhancing the security of its digital infrastructure and fostering innovation in artificial intelligence. The Home Ministry’s National Cyber Crime Reporting Portal has registered a significant rise in cybercrime complaints, with 7,000 daily complaints from January to May 2024, primarily related to online financial fraud.

Globally, India continues to face a high volume of cyberattacks. In the second quarter of 2024, India-based institutions experienced the second-highest number of weekly attacks, per organisation, in the Asia Pacific region. The increased budget aims to address these vulnerabilities and bolster India's defences against cyber threats.

MAHARASHTRA LAUNCHES CYBERCRIME HELPLINE

On 25 July 2024, Maharashtra introduced a new helpline, 9019115115, designed to enhance cybercrime awareness which is supported and managed by the "What Now" movement in partnership with the Maharashtra Yuva Cyber Suraksha Upkram. The helpline aims to strengthen the state's response to cybercrime.

This initiative is part of broader efforts to improve Maharashtra's cybercrime prevention and response systems. The "What Now" movement, co-founded by Neeti Goyal and Nivedita Shreyansh, focuses on educating young people about cybersecurity and assisting cybercrime victims.

Key figures who attended the launch event at Yashwantrao Chavan Pratishthan Hall, including Vivek Phansalkar, Mumbai's Commissioner of Police, and B K Singh, Director-General of Maharashtra State Security Corporation.

The new helpline complements the existing cybercrime helpline 1930, providing an additional resource for reporting online fraud and seeking assistance. The state is also establishing a new cybersecurity centre in Mahapay to further enhance its cybercrime response capabilities.

IFF HOSTS ROUNDTABLE ON OFFSHORE BETTING AND GAMBLING

India Future Foundation (IFF), in collaboration with Rashtriya Raksha University (RRU), India, hosted a Roundtable Conference on **'Implications of Illegal Offshore Betting and Gambling on National Security,'** on 5 July 2024, at India Habitat Centre, New Delhi.

This consultation brought together distinguished experts from the government, industry and the academia, which addressed the multifaceted challenges posed by illegal offshore betting and gambling platforms. Discussions at the consultation focused on threat to national security threats, economic impact, societal harm and the need for a unified regulatory framework to tackle these issues effectively.

Highlights of the Event

Col Nidhish Bhatnagar (Retd), Managing Director, Security and Scientific Technical Research Association (SASTRA), Rashtriya Raksha University, set the stage by outlining the significance of the topic and the urgent need for collaborative efforts to address the threats posed by illegal betting and gambling.

Mr Rakesh Maheshwari, Former Group Coordinator of the Cyber Laws Division, Ministry of Electronics and Information Technology, provided an insightful overview of the online gaming market in India. He highlighted ongoing government initiatives to combat the menace of illegal betting and gambling, emphasising on the importance of robust legal and technological frameworks.

OUR EVENTS

Our Chief Guest, **Maj Gen Manjeet Singh,** Joint Secretary (Cyber), National Security Council Secretariat (NSCS), who underscored the growing influence of illegal betting and gambling platforms and the critical need to take stringent steps to curb their rise. He emphasised that these platforms directly threaten national security and undermine the country's economic stability and societal well-being.

The report **“Curbing Betting and Gambling in India: A National Security Imperative”** was launched by Col Bhatnagar. The report provided comprehensive insights into risk emanating from illegal betting and gambling risks and proposed actionable recommendations for policymakers and stakeholders.

Vivan Sharan, Partner, Koan Advisory, discussed the necessity of establishing a registration framework for online gaming intermediaries. He advocated for a unified regulatory authority to oversee and regulate the industry, ensuring transparency and accountability.
Col Sanjeev Relia (Retd), Chief Strategy Officer, Athenian Tech Private Limited, concluded the event by summarising the key takeaways and reiterating the collective responsibility to address the challenges posed by offshore betting and gambling platforms.

Col Sanjeev Relia (Retd), Chief Strategy Officer, Athenian Tech Private Limited, concluded the event by summarising the key takeaways and reiterating the collective responsibility to address the challenges posed by offshore betting and gambling platforms.

IFF HOSTS DISCUSSION ON ENHANCING CYBERSECURITY IN ONLINE GAMING

India Future Foundation (IFF) successfully hosted an exclusive roundtable discussion on **“Online Gaming: Enhancing Cybersecurity and Data Privacy”** on 24 July 2024, at the India Habitat Centre, New Delhi.

This landmark event brought together representatives from the government, industry, academia and law enforcement agencies who addressed the pressing need for having in place robust cybersecurity measures and data privacy protocols in the burgeoning online gaming sector.

The discussions at the consultation was enriched with insightful contributions highlighting the exponential growth of the online gaming industry in India and the significant challenges in ensuring user safety and privacy.

Key topics, discussed at the consultation, included cybersecurity in online gaming, importance of data privacy, and the implications of the Digital Personal Data Protection (DPDP) Act 2023, on the sector.

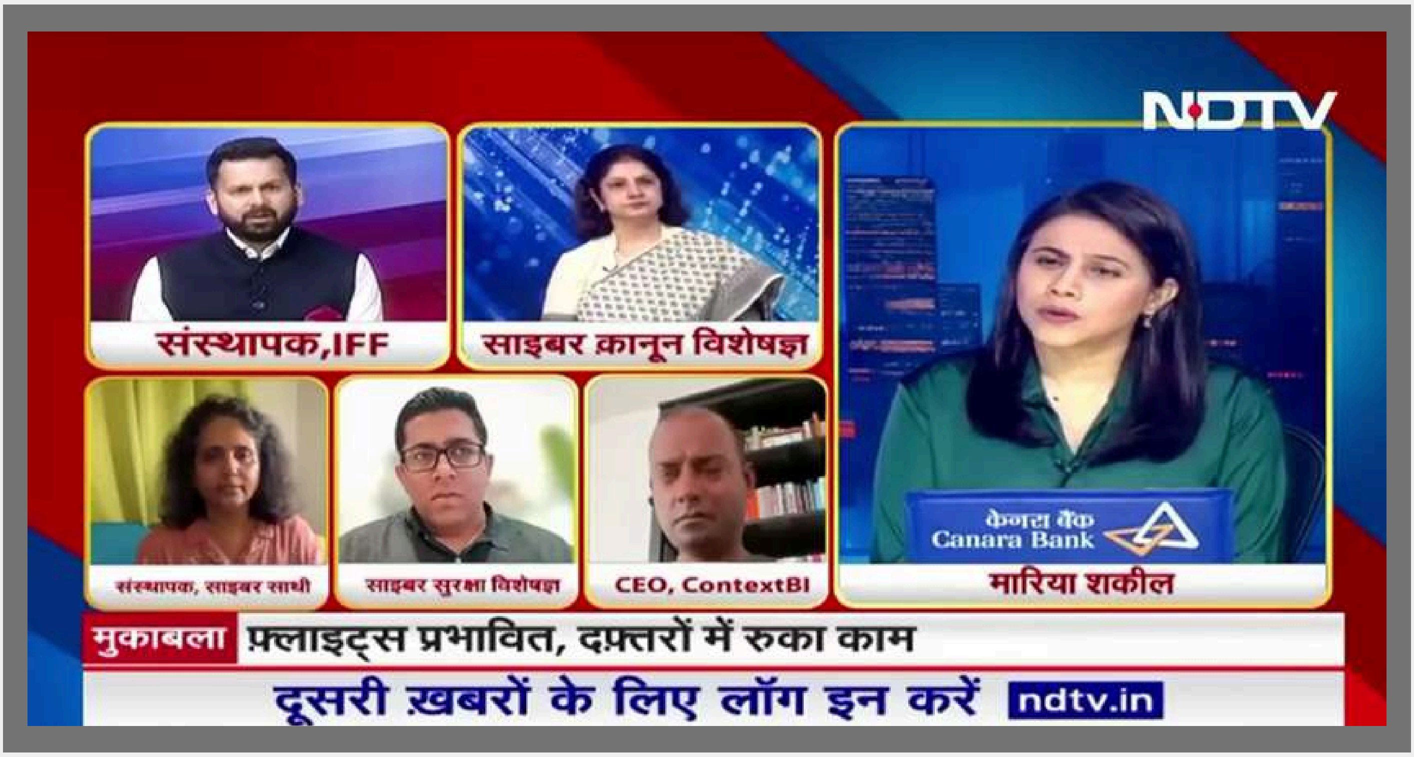
OUR EVENTS

IFF was privileged to have representatives from the Ministry of Electronics and Information Technology, representatives from law enforcement agencies and leading academic institutions like the Indian Institute of Public Administration and NLU, Delhi. Their valuable insights and expertise paved the way for a comprehensive roadmap to safeguard users and foster a secure gaming environment, ultimately contributing to our country's economic growth.

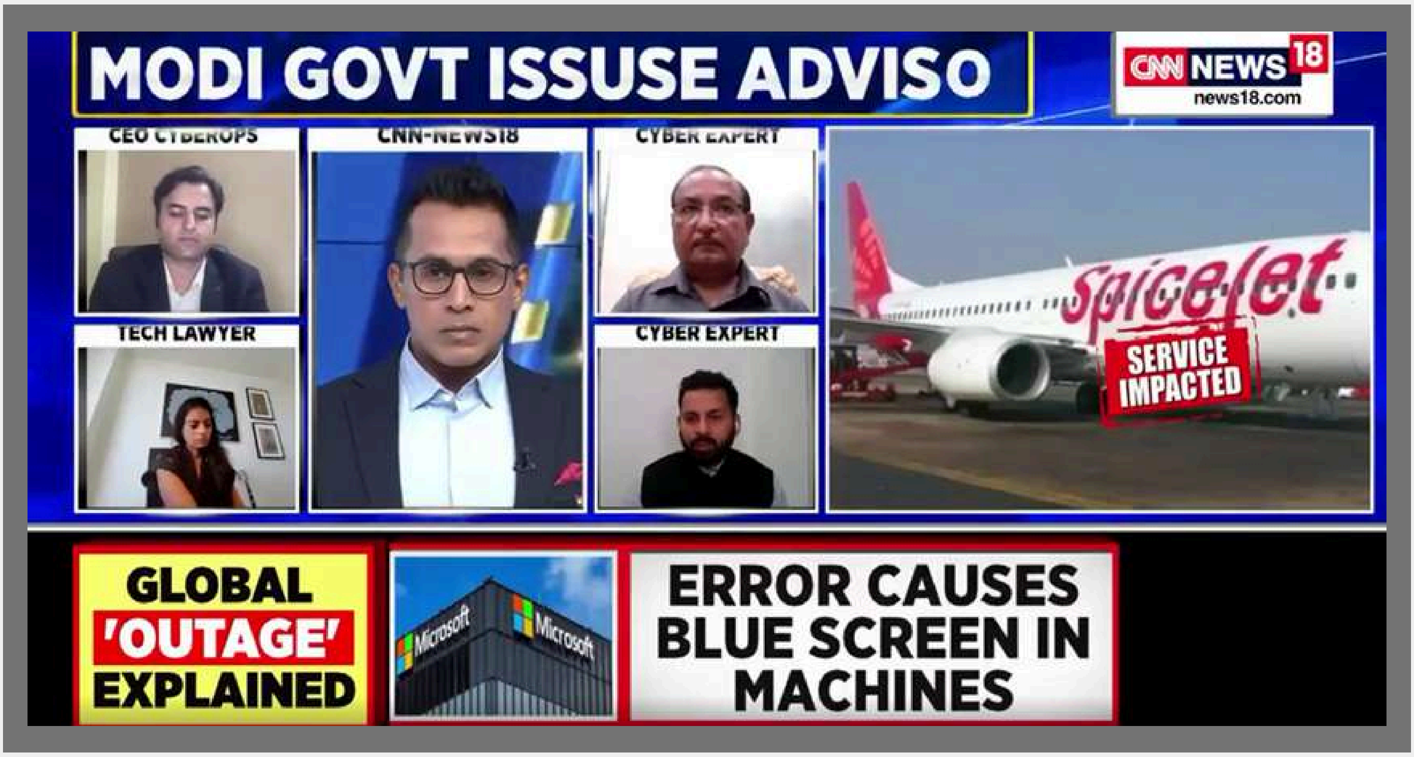
Key Takeaways

- Enhanced strategies for improving cybersecurity in online gaming
- The critical role of data privacy in protecting users
- Collaborative efforts are needed from all stakeholders to build a safer gaming ecosystem

IFF IN THE MEDIA

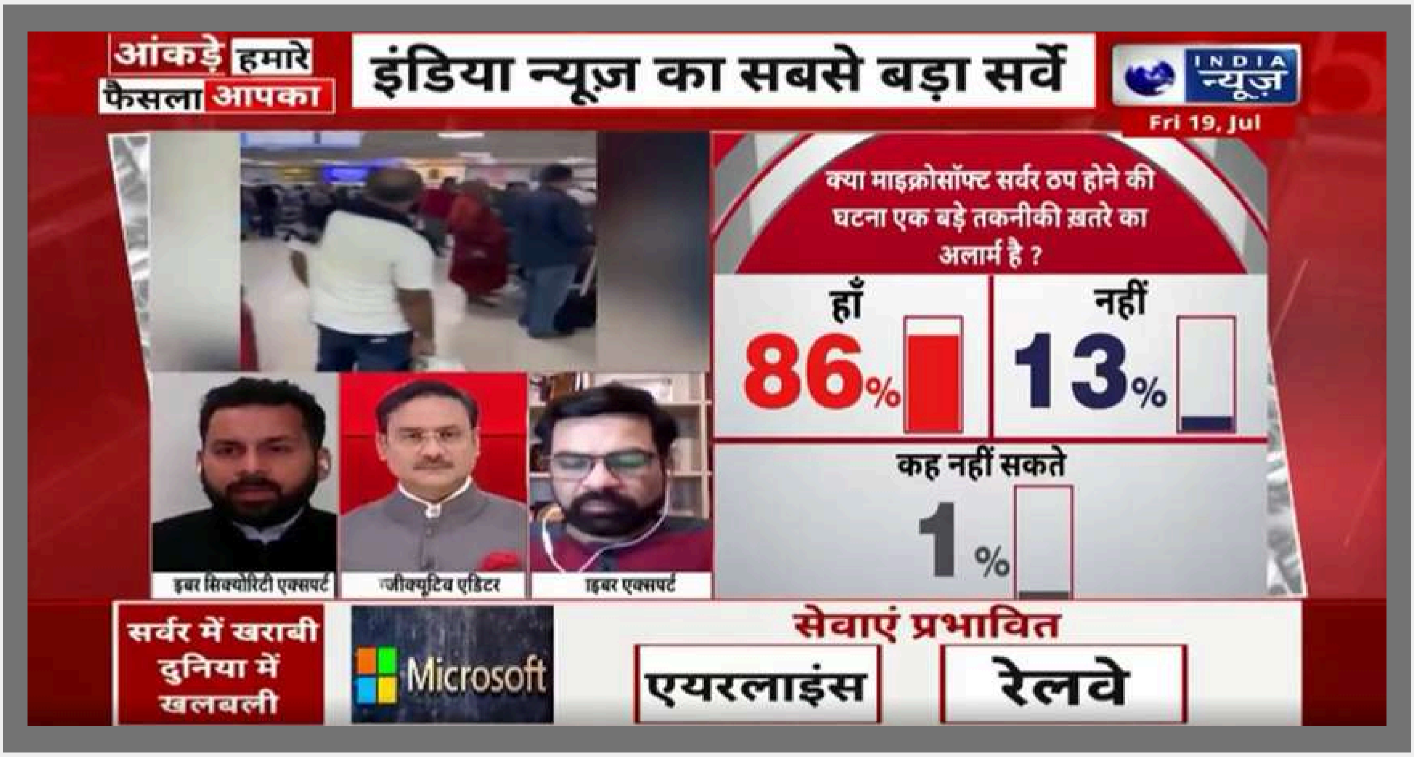


Kanishk Gaur, Founder & CEO, IFF, spoke with *NDTV India* on why India should build stronger partnerships with companies like CrowdStrike and Microsoft instead of replacing them.

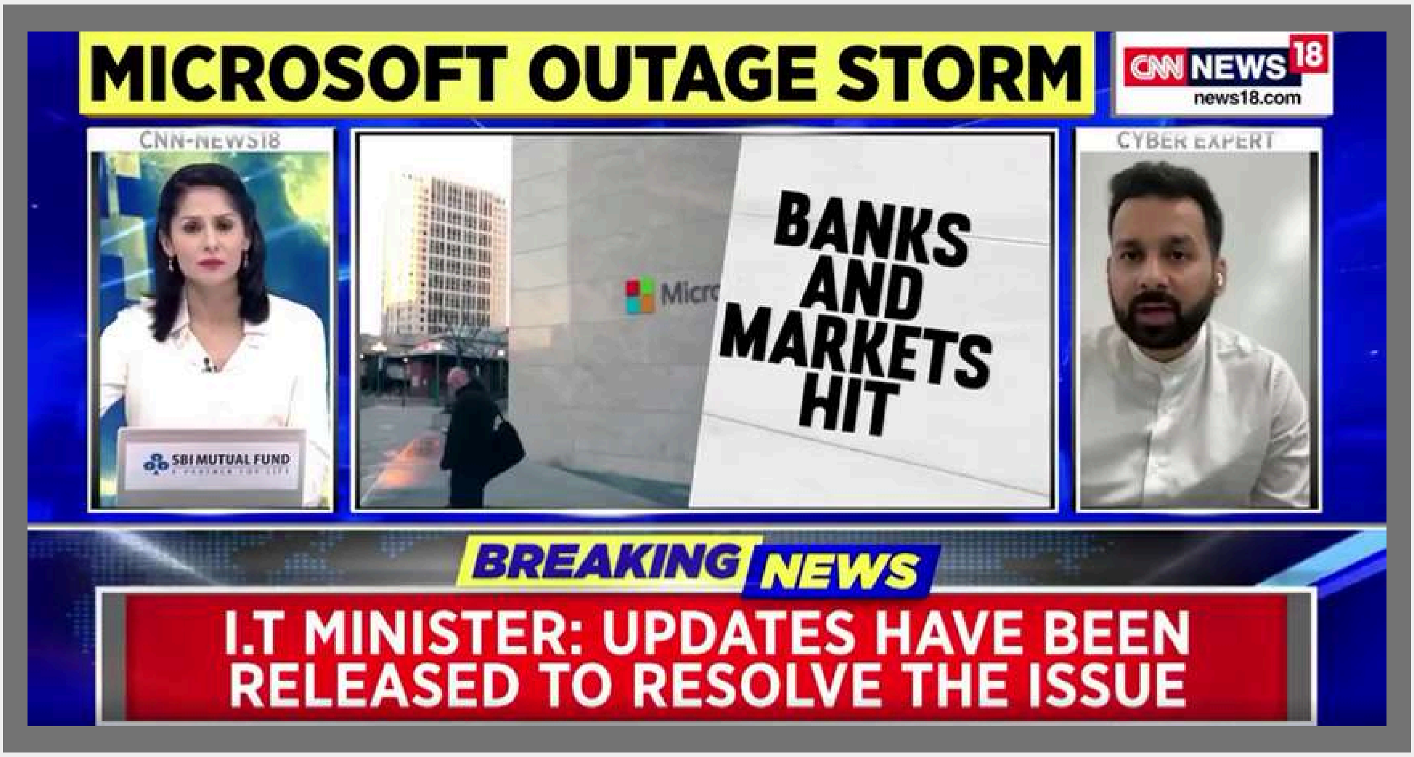


Kanishk Gaur, Founder & CEO, IFF, spoke about disaster recovery and resilience strategies, in the wake of a faulty update of CrowdStrike's Falcon Agent on *CNN-News18*.

IFF IN THE MEDIA

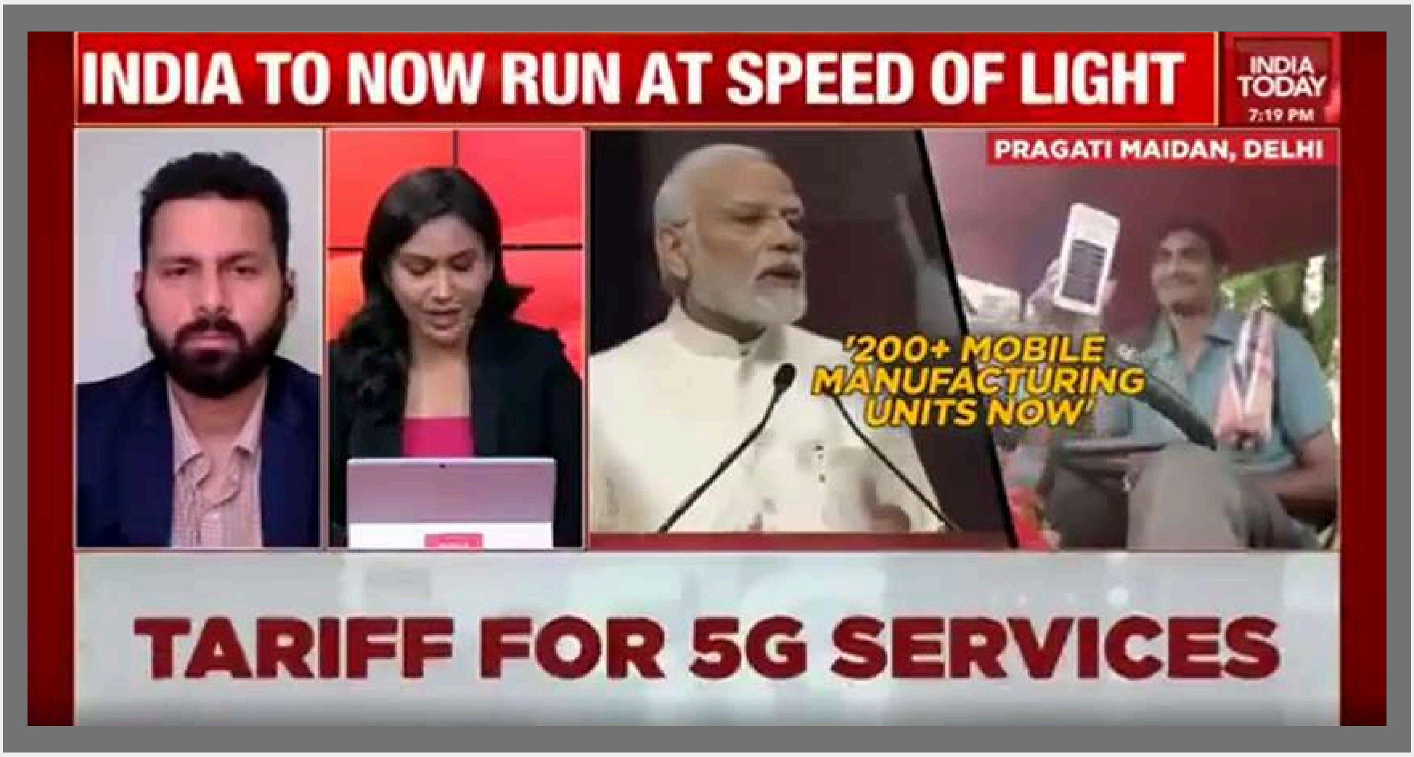


Kanishk Gaur, Founder & CEO, IFF, highlighted the critical need for robust business continuity plans following the BSOD incident with CrowdStrike Falcon Surface on *INDIA NEWS*.

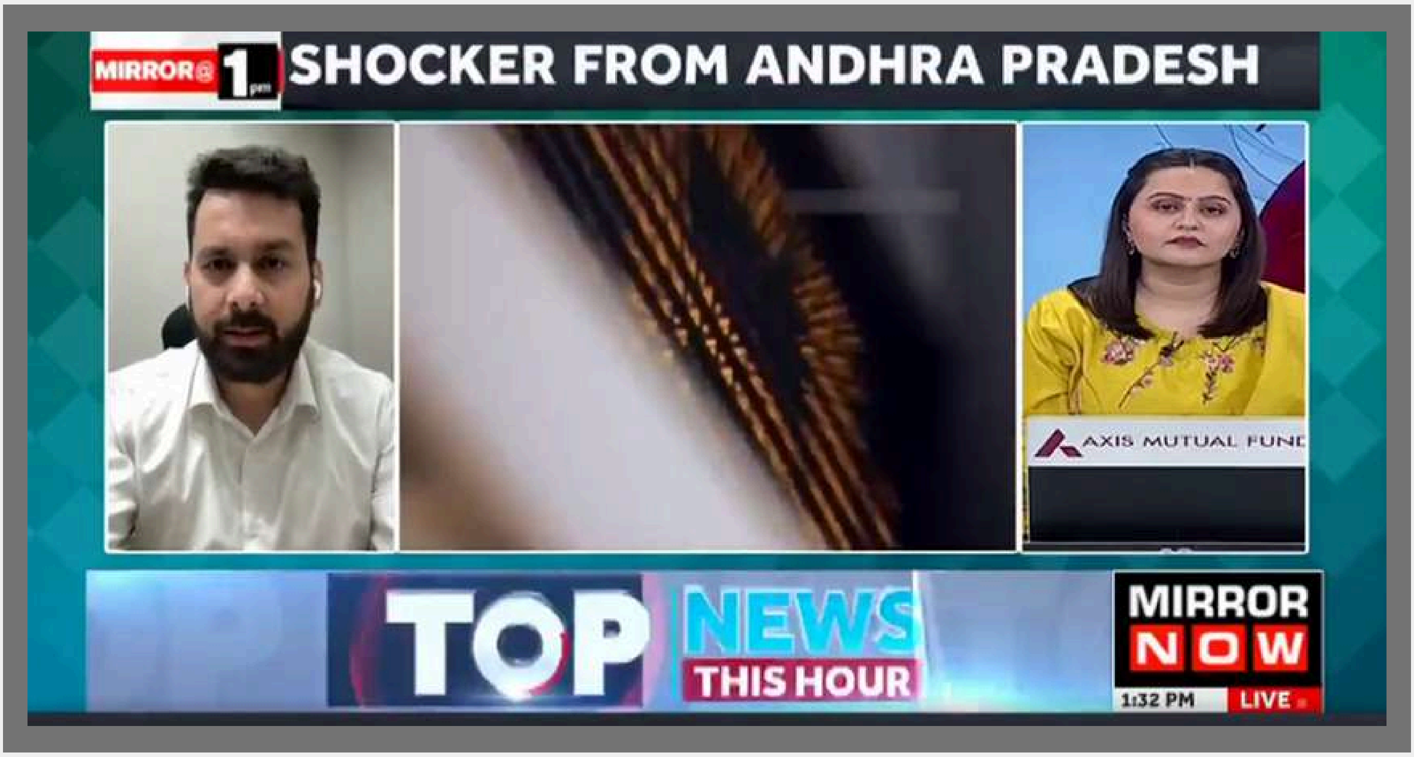


Kanishk Gaur, Founder & CEO, IFF,
spoke about the BSOD impacting millions of users globally, with *CNN-News18.*

IFF IN THE MEDIA

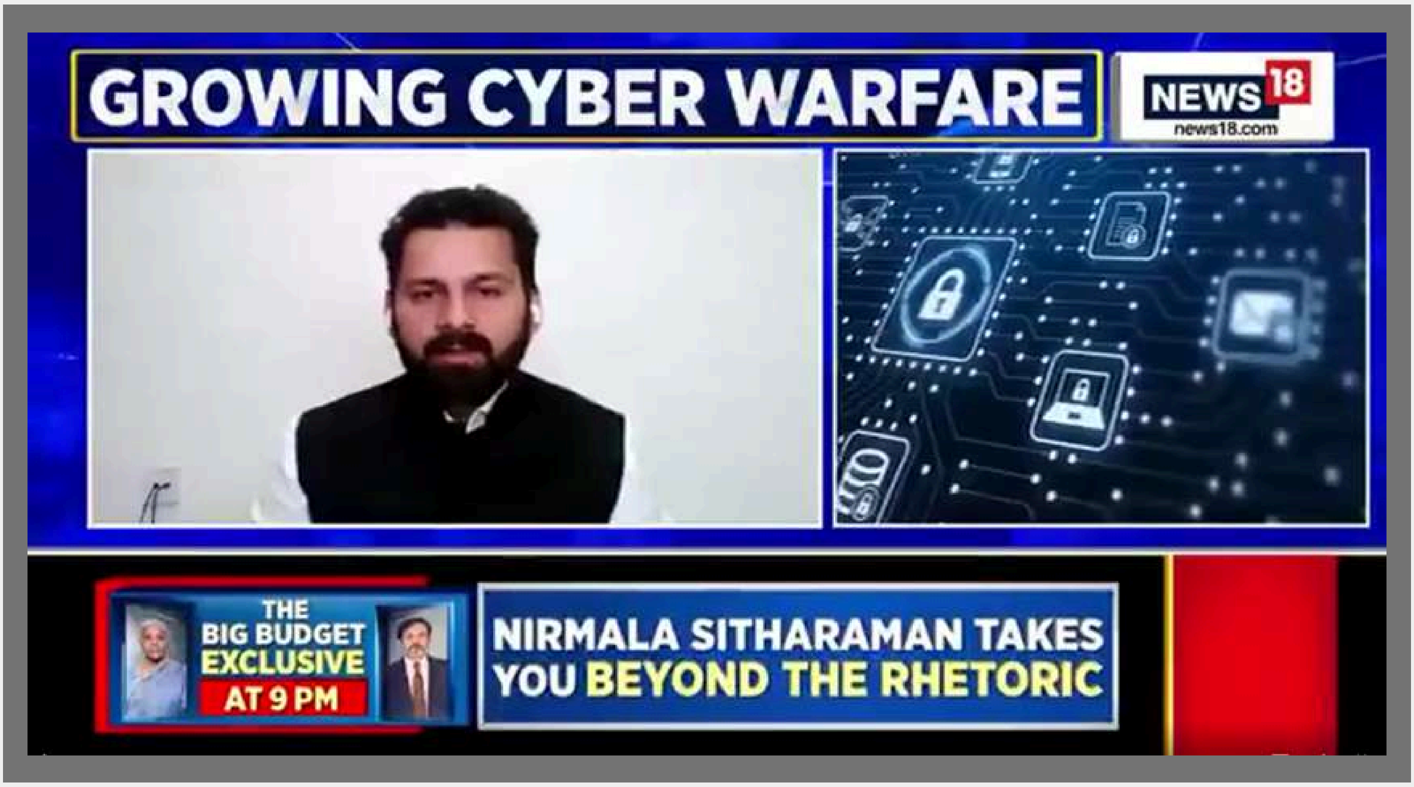

INDIA TO NOW RUN AT SPEED OF LIGHT
INDIA TODAY
7:19 PM
PRAGATI MAIDAN, DELHI
'200+ MOBILE MANUFACTURING UNITS NOW'
TARIFF FOR 5G SERVICES

Kanishk Gaur, Founder and CEO, IFF,
shared his insights on 5 G's transformative potential with *India Today*.



Kanishk Gaur, Founder & CEO, IFF,
addressed the impact of social media trolling and bullying on *Mirror Now*.

IFF IN THE MEDIA


GROWING CYBER WARFARE
NEWS 18
news18.com
THE BIG BUDGET EXCLUSIVE AT 9 PM
NIRMALA SITHARAMAN TAKES YOU BEYOND THE RHETORIC

Kanishk Gaur, Founder & CEO, IFF,
discussed the surge in cybersecurity attacks targeting India on *CNN-News18*.

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