INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

NEWS FROM AROUND THE WORLD

INCREASING CYBERSECURITY ATTACKS IN INDIA

According to a report by Palo Alto Networks, rapid advancements in technology is leading to a surge in cyberattacks in India. Prominent among the sectors that are at the receiving end of the such attacks is the government and the private sector.

The report, released on 11 September 2023, highlights the fact that India faces a substantial risk of cyberattacks targeting its critical infrastructure, public sector and essential services. Shockingly, the data reveals that 67 percent of the entities of the Government of India and entities engaged in providing essential services have reported encountering a surge of over 50 percent in disruptive cyberattacks.

Manufacturing, logistics, and the Banking, Financial Services, and Insurance (BFSI) sectors stand out among the sectors facing the most significant threats from cyberattacks. The report shows that 66 per cent of Indian manufacturing firms have faced increased risks from unsecured IoT devices connected to their networks, which is far more than other sectors. Additionally, 50 per cent of these manufacturing organizations believe that adopting 5G technology will further widen the security loopholes.

IN THIS NEWSLETTER

1. News From Around the World 01

2. Our Events 14

3. IFF in the Media.....15

Cyberattacks have also significantly impacted organisations in the transport and logistics sectors, with 83 per cent of entities in this sector perceiving their risk level as high or very high. The banking and financial sectors are not spared either, with 34 per cent of Indian organizations in this domain expressing concerns that cloud attacks will disrupt their businesses.

As per the report, one of the critical factors that has contributed to the increase in cyberattacks, in the country, is the rapid advancement of technologies. According to the report, 69 per cent of Indian telecommunications companies (Telcos) have faced newfound risks due to increased reliance on cloud-based services and applications. Additionally, 57 per cent of Indian Telcos are worried about the growing threat of ransomware attacks.

The report further noted that, in response to the growing menace of cyberattacks, Indian organizations are reallocating their budgets to give priority to their cybersecurity requirements. The report reveals that 94 percent of Indian organizations regularly perform assessments and forensics for operational technology (OT) related cybersecurity incidents. Moreover, 89 percent of these organizations have IT and OT cybersecurity professionals working together in the same team, surpassing the Southeast Asia average of 82 percent.

As India progresses in the digital age, the need for a proactive and comprehensive approach to cybersecurity has never been more crucial, than ion the present day. The report by Palo Alto Networks serves as a stark reminder of the evolving threats that organizations and government entities must confront in this increasingly connected world.

CYBERSECURITY ADVISORY: ALERT AA23-270A

The United States National Security Agency (NSA), the U.S. Federal Bureau of Investigation (FBI), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Japan National Police Agency (NPA), and the Japan National Center of Incident Readiness and Strategy for Cybersecurity (NISC) have jointly released a cybersecurity advisory on 27 September 2023 to address the activities of the People's Republic of China (PRC)-linked cyber actors: BlackTech. These actors have shown the ability to modify router firmware without detection and exploit routers' domain-trust relationships, focusing on international subsidiaries and headquarters in Japan and the U.S.

BlackTech has been active since 2010, targeting many public organizations and private industries in the U.S. and East Asia. Their tactics include developing custom malware and persistence mechanisms for compromising routers, allowing them to pivot between international subsidiaries and domestic headquarters networks.

BlackTech actors employ custom malware payloads and remote access tools (RATs) to target the victim’s operating systems. These actors utilize a range of custom malware families to evade detection by security software. They also use stolen code-signing certificates to make malicious payloads appear genuine.

Living off-the-land tactics allow BlackTech actors to blend in with normal network activities, making it challenging for endpoint detection and response products to detect their presence.

BlackTech actors typically target the international subsidiaries of U.S. and Japanese companies. After gaining access to the subsidiaries' networks, they exploit trusted relationships to pivot between the subsidiaries and the headquarters.

It has also been seen that BlackTech actors target various brands and versions of router devices, enabling them to conceal configuration changes, hide commands and turn off logging while conducting operations. They often modify router firmware to conceal their activity and maintain persistence. They may also replace the firmware for certain routers, establishing persistent backdoor access and obfuscating their activity.

To detect and mitigate BlackTech's malicious activity, several recommendations are provided. These include the following.

- Disable outbound connections on virtual teletype (VTY) lines.
- Monitor both inbound and outbound connections from network devices.
- Limit access to administration services and only permit specific IP addresses.
- Upgrade to devices with secure boot capabilities and prioritize replacing end-of-life equipment.
- Change all passwords and keys if a single password is compromised.
- Review logs for unauthorized changes to configuration or firmware.
- Periodically perform file and memory verification to detect unauthorized changes.
- Monitor for changes to firmware and take snapshots periodically.

Implementing these measures can help defend against BlackTech's cyber activities and protect network infrastructure from their malicious actions.

MAHARASHTRA'S RS 837 CRORE CYBERSECURITY PROJECT

On 6 September 2023, the Maharashtra Cabinet approved the implementation of a cybersecurity project with an estimated cost of Rs 837 crore to combat the rising instances of cybercrimes, in the state. The project aims to equip the State with advanced technologies, a skilled workforce and essential resources to effectively address and mitigate cyber threats, ultimately transforming Maharashtra into a "cyber-safe" state.

Once operational, this initiative will establish a 24/7 call centre that will enable citizens to register their complaints related to cybercrimes through phone calls. These complaints will undergo thorough investigations, leveraging cutting-edge cybersecurity technology to promptly identify and address cyber threats.

MAHARASHTRA'S RS 837 CRORE CYBERSECURITY PROJECT

A report compiled by Cloudflare, a company specializing in security, has unveiled alarming statistics, indicating that 83 per cent of Indian organizations have faced at least one cybersecurity incident in the past year. For nearly half of these entities (48 per cent), the impact was severe, as they had to contend with ten or more incidents, which resulted in losses of millions of dollars.

The respondents noted that the primary motivation of cybercriminals, behind the attacks, was financial gain, followed by spyware planting and data exfiltration. The survey covered 4,009 decision-makers and cybersecurity leaders from organizations of various sizes, including small (150 to 999 employees), medium (1,000 to 2,500 employees) and large (over 2,500 employees).

A concerning finding from the study is that only 52 per cent of the surveyed organizations considered themselves to be highly prepared to handle cybersecurity incidents. Lack of preparedness came at a high cost, with 47 per cent reporting financial losses exceeding $1 million in the past year. An additional 27 per cent suffered financial setbacks of no less than $2 million.

The impact of these incidents extended beyond financial losses, as 46 per cent of the organizations experienced operational disruptions, resulting in restricted hybrid work, employee layoffs and postponed expansion plans.

The report also emphasized on the challenges organizations face in establishing their cybersecurity readiness. A significant 57 per cent of Indian business leaders identified lack of talent as their most substantial obstacle, while 44 per cent citing insufficient funding as a hindrance to safeguarding their businesses.

These findings underscore the critical importance of robust cybersecurity measures in the digital age and highlight the need for organizations to invest in talent and resources to protect themselves in an evolving landscape of cyber threats.

INDIAN HACKERS TARGET CANADA'S GOVERNMENT

In the last week of September, Canadian Federal institutions faced cyberattacks, reportedly orchestrated by an Indian hacker group.

The target of these attacks included the websites of Canada's Armed Forces and the House of Commons. Despite these attacks, Canada's counter-intelligence agency had indicated that the intrusions were a "nuisance" and did not pose a significant risk to private information.

These cyberattacks come at a time of increased tensions between Canada and India, sparked by Canadian Prime Minister Justin Trudeau's claims of "credible allegations" of Indian involvement in the killing of Sikh independence activist Hardeep Singh Nijjar in British Columbia in June 2023.

The cyber incidents serve as a reminder of the growing significance of cybersecurity in international relations and the need for vigilance in protecting government and public institutions from cyber threats.

EU SEEKS DETAILS ON CHINA'S DATA AND ANTI-SPYING LAWS

Vera Jourova, Vice President, The European Commission has expressed concerns about the lack of clarity in China's new data and anti-espionage laws. European businesses dealing with China are worried about the ambiguity in these regulations, which were expanded in July 2023. Of particular concern is the absence of clear definitions for terms like national security and national interests.

China's anti-espionage law has created uncertainties for foreign companies operating in the country. For instance, the law bans the transfer of any information related to national security and interests without providing specific definitions for these terms. The European Commission is now seeking further details from Chinese authorities to help European businesses understand the law better and ensure compliance.

The extended definition of espionage to include cyberattacks against state organizations or critical infrastructure has added complexity and ambiguity to the situation. European businesses also seek assistance in streamlining and expediting the lengthy procedural processes required for compliance.

SHORTAGE OF CYBERSECURITY PROFESSIONALS IN THE EU

The European Union Agency for Cybersecurity (ENISA) has announced significant progress in implementing and adopting the European Cybersecurity Skills Framework (ECSF) at the second European Cybersecurity Skills Conference that was held between 21-22 Sep 2023. With new legal requirements and growing threats, the demand for cybersecurity professionals in the European Union (EU) has risen sharply. While the number of cybersecurity graduates has increased to 3,100, which is a 25% growth in the past two years over the preceding two years. Still the estimated workforce shortage remains of 300,000. The conference discussed the importance of addressing this shortage through reskilling and upskilling efforts and how the ECSF is being applied to harmonize the approach across member states and sectors.

ENISA's Executive Director, Juhan Lepassaar, emphasized the need for human capital to meet EU's cybersecurity requirements. The conference also highlighted new pledges and initiatives contributing to a larger cybersecurity workforce and announced the review of the ECSF which serves as the EU reference point for defining and assessing relevant skills, as outlined in the Cybersecurity Skills Academy that was recently announced by the European Commission. The ECSF summarises the cybersecurity-related roles into 12 profiles, which are individually analysed into the details of their corresponding responsibilities, skills, synergies and interdependencies.

US AIR FORCE CANCELS EC2 CONTRACT

The US Air Force has taken the unexpected step of cancelling a significant cybersecurity technology solicitation valued at a minimum of $5 billion. The Enterprise Cyber Capabilities (EC2) contract competition, launched more than 18 months ago, had to be halted due to the staggering number of proposals submitted by private sector entities and in a notice posted on SAM.gov, the Air Force stated that the cancellation was a carefully considered decision, driven by the practical challenges of evaluating such a large volume of proposals. While the US Air Force recognized the positive outcome of substantial industry interest, it concluded that the acquisition strategy and evaluation methodology were not designed to handle many prime contract awards. The notice stressed that the cancellation was made in the best interest of the Air Force and the private sector, avoiding an unmanageable situation where more contracts would be awarded than could be properly administered.

Key Points:

Overwhelming Response: The US Air Force received an unexpectedly high number of proposals, with over 250 submissions from companies in the private sector, thereby making the entire competition unmanageable.

Cancellation Justification: The US Air Force's decision to cancel the competition, was guided by a commitment to suit the best interests of the government and the private sector. The existing acquisition strategy and evaluation methodology were unsuitable for dealing with the overwhelming response.

Intended Use of EC2 Contract: Originally, the EC2 contract was intended for applications in areas such as command and control, planning and operations, vulnerability research, full-spectrum testing, software development, tool development, modeling, simulation, and threat assessment.

Timeline: The solicitation process began in March 2022 with the release of a pre-solicitation announcement. After six months, the final solicitation was published, and the deadline for proposal submissions was in January 2023. The Air Force indicated it was in the source selection phase before the contract was canceled.

Implications for Companies: Businesses working on proposals for the EC2 contract invested considerable time and resources over two years, incurring costs amounting to hundreds of thousands of dollars.

Future Strategy: The US Air Force is exploring alternative approaches to meet its original cybersecurity requirements, which were initially intended to be addressed by the EC2 contract. These options may involve issuing a new solicitation or using an existing procurement vehicle.

Cancelling the EC2 contract signifies the challenges in managing an unexpectedly high number of proposals in competitive procurement processes, impacting both the government and the private sector. The Air Force is seeking alternative solutions to fulfill its cybersecurity requirements effectively.

INTERNATIONAL CRIMINAL COURT CYBERSECURITY INCIDENT

On 19September 2023, The International Criminal Court (ICC), The Hague, Netherlands, detected an "anomalous activity" affecting its systems. While the ICC did not provide details of the incident, it confirmed that immediate measures have been taken in response to the incident. It needs to be noted that the incident has not disrupted the core functions of the Court.

In a notable case from 2022, a Dutch intelligence agency had revealed that it had thwarted an elaborate attempt by a Russian spy, operating under a false Brazilian identity, to work as an intern at the Court. The ICC has been investigating allegations of Russian war crimes in Ukraine and has issued a war crimes arrest warrant for President Vladimir Putin.

In response to inquiries about the incident, the Dutch foreign ministry expressed deep concern, stating, that any malicious activities that undermine the Court's cybersecurity or interfere with its ability to fulfill its mandate safely and securely are of utmost concern.

The exact details of the incident remain undisclosed. Still, the ICC's commitment to strengthening its cybersecurity framework and the continued support from Dutch authorities reflect the determination to ensure the security and integrity of the Court's operations.

RUSSIAN HACKERS TARGET THE UKRAINIAN GOVERNMENT

Russian hackers have escalated their cyberattacks on Ukraine's law enforcement agencies to gain insights into war crimes investigations by Ukrainian authorities. Victor Zhora, the Deputy Chairman of Ukraine's cybersecurity service (SSSCIP), revealed about these espionage campaigns during a press conference. It remains unclear whether these attacks were successful or if they compromised sensitive information related to war crimes investigations.

Since the conflict's inception in February 2022, Ukraine has collected evidence of Russian war crimes, including allegations of civilian killings, rape, hostage-taking, torture and civilian infrastructure bombing. This information is crucial for the prosecution of alleged war criminals.

According to SSSCIP's latest report, Russian hackers are potentially seeking list of war crime suspects to help evade prosecution. They are also interested in determining which elite soldiers and officers may have been captured in Ukraine and whether they can be exchanged. This evidence could be invaluable for the Kremlin for various purposes.

In September, the International Criminal Court (ICC) established a field office in Kyiv, emphasizing its commitment to investigating Russian war crimes. The ICC has also indicated its intention to treat cyber incidents as potential war crimes. This shift highlights the significance of Russia's cyberattacks on Ukraine's critical civilian infrastructure.

Moreover, Russian hackers have been targeting victims who have been compromised in the past, leveraging prior knowledge of the victim organization's network infrastructure, defensive measures, key personnel and communication patterns.

As Ukraine faces the upcoming winter season amidst the persistent threat of blackouts and escalating missile strikes, Zhora warned of potential Russian cyberattacks on the country's vital infrastructure, including energy facilities. SSSCIP is prepared to safeguard these critical assets, as it gained greater authority over its cybersecurity defences last year.

This development signifies the ongoing cyber warfare between Russia and Ukraine and critical role of cyberattacks in shaping the conflict's course.

CHINA'S AI-POWERED INFLUENCE OPERATIONS

China has introduced a new cyber capability driven by artificial intelligence (AI) that automatically creates images for influence operations. These operations are designed to imitate US voters representing various political ideologies, sparking racial, economic and ideological controversy.

The Microsoft Threat Analysis Center (MTAC) published a report titled "Sophistication, Scope, and Scale: Digital Threats from East Asia Increase in Breadth and Effectiveness," revealing the growing threat of influence operations and cyber activities in the East Asia region.

China-linked entities employ AI-generated media to target politically divisive subjects such as gun violence and disparage US political figures and symbols. This technology surpasses previous campaigns by producing compelling content, although the extent and scale of its deployment remain uncertain.
Microsoft emphasized the urgency of addressing the weaponization of AI technology by cyber and influence threat actors.

China-affiliated threat actors have also been observed carrying out cyber operations focused on the South China Sea region, with targets including regional governments and industries. They have also shown interest in the US defence industry and infrastructure. Notably, a China-based threat actor known as Storm-0558 gained unauthorized access to Microsoft customer email accounts from approximately 25 organizations, thereby suggesting espionage motives.

China is globally engaged in state-sponsored propaganda efforts to bolster its international image. Over 230 state media personnel and affiliates pose as independent social media influencers, disseminating Chinese Communist Party (CCP) propaganda to a collective audience of 103 million people across 40 languages on Western social media platforms.

Unlike Iran and Russia, China has not yet merged cyber and influence operations. Meanwhile, North Korea primarily focuses on intelligence gathering and cryptocurrency theft. The maritime and shipbuilding sectors are prominent targets, with recent espionage activities directed at the Russian government and the defence industry, accompanied by support for Russia in the Ukraine conflict.

The report, published by Microsoft, anticipates escalating threats from China and North Korea, particularly concerning Taiwan and the United States of America, in the lead-up to the 2024 elections in Taiwan and the USA.

Cross-industry collaboration is essential to confront these challenges, as nation-state actors persist in exploiting vulnerabilities and disseminating detrimental narratives globally.

CHINA'S AI-POWERED INFLUENCE OPERATIONS

China's Ministry of State Security (MSS) has alleged that the United States of America has been conducting extensive cyber espionage operations against numerous countries, including China, with a focus on surveillance, stealing data and implanting backdoors on servers since 2009, amidst escalating geopolitical tensions between the two nations.

The government authority used WeChat to release a statement accusing U.S. intelligence agencies of employing a formidable cyberattack arsenal to engage in systematic cyberattacks, secret theft and intrusions at a global scale. Although specific details about these alleged hacking activities were not provided, the MSS singled out the U.S. National Security Agency's (NSA) Computer Network Operations as a unit that had carried out platform-based attacks against China over the years, aiming to exploit the nation's crucial data resources.

The statement also claimed that in 2009 the NSA hacked into Huawei's servers and has since conducted "tens of thousands of malicious network attacks" against domestic organizations, such as the Northwestern Polytechnical University, Xi'an, China. These attacks were allegedly aimed at extracting sensitive data, a charge initially raised by China in September 2022.

Moreover, China's National Computer Virus Emergency Response Centre (NCVERC) reportedly uncovered a spyware artifact known as Second Date while responding to an incident at a public research university. This malware, allegedly developed by the NSA, operates covertly on "thousands of network devices in many countries around the world" and can monitor, hijack network traffic and inject malicious codes. Several countries, including Germany, Japan, South Korea, India, and Taiwan, are believed to be targets of this spyware.

The MSS contends that U.S. intelligence agencies have been conducting cyberattacks and cyber espionage for over a decade against 45 countries and regions, including those in China and Russia, focusing on sectors such as telecom, scientific research, economy, energy and the military.

In addition, the statement accuses the U.S. of pressuring technology companies to insert backdoors into their software and equipment to facilitate cyber espionage and data theft. The MSS references companies like X-Mode Social and Anomaly Six, which are believed to be able to track users' mobile phones.

The MSS characterizes the U.S. as a long-standing practitioner of large-scale eavesdropping on countries worldwide, including its allies, while presenting itself as a victim of cyberattacks. The US is accused of persuading other nations to join its "clean network" initiative in the name of network security to exclude Chinese firms from the global network market.

This revelation follows an incident in July 2023, when Microsoft disclosed a cyber espionage campaign by a China-linked actor, codenamed Storm-0558, targeting two dozen organizations in the United States and Europe. China responded by labeling the US as the "world's biggest hacking empire and global cyber thief."

The MSS, which made its WeChat debut on 1 August 2023, has emphasized on the importance of strengthening counter-espionage efforts and encouraging citizens to report suspicious activities, with the promise of rewards and protection for their contributions.

ROLE OF HR IN CYBERSECURITY

In a rapidly evolving cybersecurity landscape that is marked by sophisticated threats, safeguarding on organisation’s critical assets extends beyond the traditional roles of Chief Information Security Officers (CISOs) and Chief Security Officers (CSOs). Human Resources (HR) department now plays a pivotal role in enhancing cybersecurity and establishing effective insider threat programmes.

Cyber threats have become more complex and dangerous, with cybercriminals, state-sponsored hackers and even disgruntled employees increasingly employing sophisticated methods to achieve their goals. Insider threats, in particular, pose a growing concern as they originate from individuals with legitimate access to systems, making it a challenging task to detect them. Technical solutions like User Entity Behaviour Analysis (UEBA) are essential for addressing these threats. Still, HR can provide valuable support through their expertise in personnel management, organizational behaviour and corporate culture. Understanding and analyzing human behaviour can lead to actionable intelligence for anticipating, identifying and mitigating human-related cybersecurity risks.

The HR department makes visible contributions to an organization’s cybersecurity by shaping talent acquisition and development strategies. By fostering an environment of creativity and innovation, HR teams contribute, in their own way, towards the fight against evolving cyber threats. Moreover, the HR department is vital in cultivating a positive security culture within the organization. It involves conducting training and awareness programmes to ensure that employees understand their roles in safeguarding the organization, its stakeholders and customers. Effective communication builds a proactive, sustainable, security-focused mindset among employees, enhancing collaborative cybersecurity defence strategies.

From an employment perspective, HR ensures compliance with applicable laws and regulations, fostering a fair and a legally compliant working environment. HR's involvement extends to collaborating on developing and enforcing robust security policies and procedures, which are integral to any security strategy.

The HR department serves as a bridge between affected employees, the organization and various departments when addressing incidents and mitigating future risks. HR is instrumental in supporting the development and activation of security incident response plans, facilitating communication during security incidents and ensuring the well-being of incident responders. HR is also crucial in supporting investigations related to breaches or incidents with a human element.

One of HR's most critical contributions lies in developing and managing organizational insider threat programmes. The HR department serves as the initial point of contact when hiring employees and oversees re-vetting and fitness and propriety attestations to make informed decisions regarding recruitment. HR manages employee databases and coordinates with business units and IT teams for joiner, mover and leaver (JML) processes. This includes updating contractual changes and access controls to minimize the risk of unauthorized access.

Additionally, HR departments leverage their experience in developing incident response plans and investigative activities to provide people-centered remediation plans. This includes strengthening and communicating security policies, enhancing transparency and developing further training, awareness, and security measures focusing on data security and privacy.

Given their involvement in incident response and investigations, the HR can define behavioural indicators and help create threat profiles. These profiles aid in identifying and prioritizing potential insider threats based on the severity of behavioural indicators, job roles, access levels and the potential harm they can cause.

In a constantly evolving cybersecurity landscape, HR's role is no longer purely supportive; it is essential in developing comprehensive cybersecurity and insider threat strategies. Collaborative approaches that leverage tools like Security Information and Event Management (SIEM) and User Entity Behaviour Analytics (UEBA) are essential for organizational cybersecurity resilience. HR professionals' insights, skills and job roles contribute significantly to these holistic efforts, and HR's role in cybersecurity is integral to the future of cybersecurity.

GUIDE TO OT SECURITY: NIST SP 800-82 REV.3

The National Institute of Standards and Technology (NIST), the United States of America, has taken a monumental step in elevating the security of Operational Technology (OT) systems with the recent release of its Special Publication (SP) 800-82 Rev 3 titled "Guide to Operational Technology (OT) Security" in September 2023. This comprehensive guide is a game-changer, aiming to fortify the security of OT systems while accommodating their unique performance, reliability and safety demands – all of which are integral to modern IT infrastructure.

Operational Technology (OT) encompasses many programmable systems and devices that interact with or manage devices affecting the physical environment. These systems contain devices that detect, monitor, control, or directly induce changes in devices, processes and events. Notable examples of OT systems encompass industrial control systems (ICS), building automation systems, transportation systems, physical access control systems, physical environment monitoring systems and physical environment measurement systems.

SP 800-82 Rev 3 provides insights into OT and its typical system configurations. It meticulously examines the identification of common threats that can affect the organizational mission and business functions reliant on OT systems. Furthermore, it elucidates vulnerabilities frequently associated with OT and furnishes a repertoire of security safeguards and countermeasures to manage the associated risks effectively.
This latest iteration of SP 800-82 Rev 3 introduces substantial improvements and updates to its guidance. The critical revisions and enhancements encompass the following:

1. **Scope Expansion:** The scope has been broadened to encompass a broader spectrum of OT, moving beyond Industrial Control Systems (ICS).
2. **Updated Threats and Vulnerabilities:** This publication considers the most recent developments in OT threats and vulnerabilities.
3. **Enhanced Risk Management:** The document now provides updates on OT risk management, recommended practices, and architectural considerations.
4. **Current Activities in OT Security:** This revision considers the most recent developments in the realm of OT security, ensuring that the guidance remains current and pertinent.
5. **Security Capabilities and Tools:** SP 800-82 Rev3 now includes information on security capabilities and tools customized for OT.
6. **Alignment with Standards:** This document is even more closely aligned with other OT security standards and guidelines, including the Cybersecurity Framework (CSF).
7. **Tailoring Guidance:** A noteworthy addition is the introduction of new tailoring guidance for SP 800-53 Rev 5 security controls, featuring an OT overlay. This overlay offers tailored security control baselines suitable for low-impact, moderate-impact, and high-impact OT systems.

In conjunction with SP 800-82 Rev 3, NIST has curated a wealth of dedicated resources focused on OT cybersecurity. These resources are readily accessible on the Operational Technology Security website (PLESE GIVE WEBSITE url)
https://csrc.nist.gov/Projects/operational-technology-security , which serves as a valuable repository of information and tools for organizations seeking to bolster the security of their OT systems. It's a crucial resource for safeguarding critical infrastructure and defending against emerging threats in the ever-evolving cybersecurity landscape.

SEBI STRENGTHENS CYBERSECURITY AT STOCK EXCHANGES

On 5 September 2023, at the Global Fintech Fest, Jio World Centre, Mumbai Madhabi Puri Buch, Chairperson of the Securities and Exchange Board of India (SEBI), unveiled a series of strategic measures to fortify cybersecurity defences within India's stock exchanges and clearing corporations. One key initiatives on the horizon is developing a client access mechanism, allowing individuals to manage their positions directly during broker server downtime, thus ensuring the seamless operation of market transactions even in the face of technical glitches.

To further enhance cybersecurity preparedness, SEBI has proposed for all regulated entities, including stock exchanges and clearing corporations, to establish an up-to-date cyber crisis management plans. These plans aim to augment the capacity to prevent, prepare for, and respond to potential cyber incidents. At the event, Buch didn't stop at cybersecurity alone; she also emphasized on the pivotal role of artificial intelligence (AI) and fintech in reshaping the financial market landscape. AI, in particular, is poised to redefine traditional regulatory approaches, enabling a more nuanced assessment of entities' compliance with regulatory standards. In the pipeline is considering "MF Lite regulations" for passive funds, a move designed to simplify compliance and spur innovation within the sector.

Furthermore, Buch underscored AI's potential to discern finer distinctions between entities and their adherence to regulatory norms, particularly when coupled with fintech innovations. This combination promises to create a more secure and dynamic financial market environment. In conclusion, SEBI's proactive stance on cybersecurity and its move to embrace of AI and fintech technologies signals the regulator's unwavering commitment to ensuring a robust and resilient financial ecosystem. SEBI seeks to tackle evolving cyber threats, enhance market security, and promote innovation and regulatory compliance in India's financial markets through these measures.

INDIA FUTURE FOUNDATION AND WORLD AUTO FORUM PIONEERING THE FUTURE AT WAFIT SUMMIT 2023

On 16 September, 2023, an event took place in New Delhi that cloud sow the seeds of how cars work in the future. It was the 7th WAFit Summit 2023 which was jointly conducted by the India Future Foundation (IFF) and the World Auto Forum.

At the event, some of the smartest people in the car industry, like Ramsunder Papineni - President Vehere; Rakesh Maheshwari - Advisor in Cyber Regulations and Compliance and former Senior Director and General Counsel for Cyber Law and Data Governance, Ministry of Electronics and Information Technology (MeitY) and Naresh Yadav- National President, Akhil Bhartiya Panchayat Sangathan, shared their ideas. Here's what they talked about:

Personalized Driving Experience: Imagine your car knowing exactly how you like to drive and making it super comfortable for you. That's what AI is making possible, and it's not science fiction; it's the future.

Predictive Maintenance: AI can now predict when your car needs fixing before it breaks down on the road. This means your car stays safe and lasts longer.

Autonomous Vehicles: We discussed the future of self-driving cars and how AI is making it happen. It's like having a smart co-pilot that drives for you.

Supply Chain Optimization: AI is like a super-smart manager for how cars are made and delivered. It ensures everything happens at just the right time, making the car industry work even better.

Enhanced Safety Features: AI can make driving safer by helping your car avoid accidents and even keeping an eye on you while you drive.

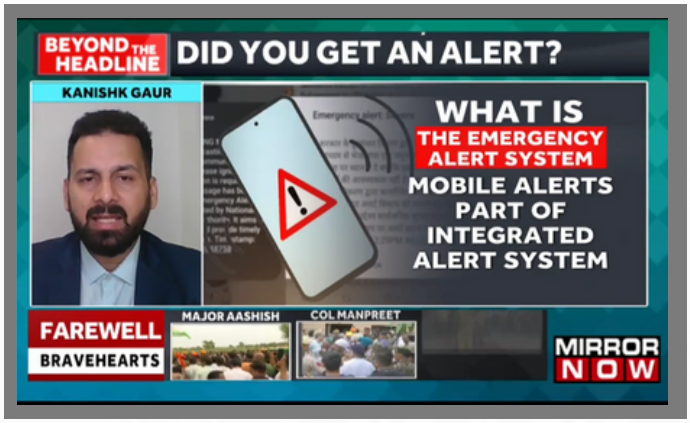
Ethical AI: We talked about the tough questions AI brings, like what happens to jobs and what the right way to use it is. It's a challenge, and we need to be careful and responsible.

The 7th WAFit Summit 2023 was like a lighthouse for new ideas, changing the future of cars. The teamwork between India Future Foundation and the World Auto Forum set a new standard for how industries can work together.

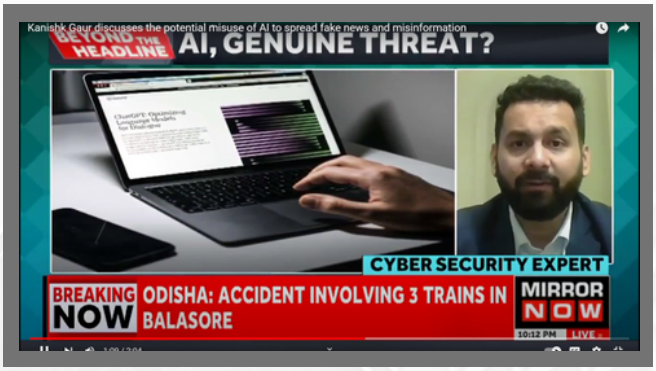
The auto industry is on the edge of a big change, and the 7th WAFit Summit 2023 showed the way. The future of how we get around is being rewritten, and it's a story of new ideas, working together, and the fantastic things AI can do.

IFF IN THE MEDIA

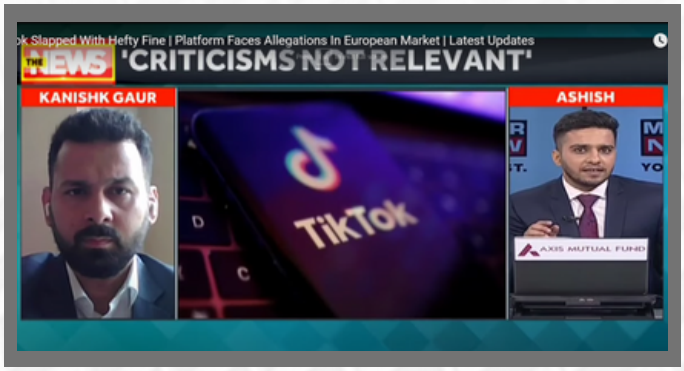
Former National Cyber Security Coordinator, Lt. Gen. (Retd) Dr Rajesh Pant joining India Future Foundation, as its Chairman covered in Tech Observer Magazine.



Kanishk Gaur, CEO, India Future Foundation, shared his insights on the Government of India's New Emergency Alert System on Mirror Now.



Kanishk Gaur, CEO, India Future Foundation, discusses the potential misuse of AI to spread fake news and misinformation on Mirror Now.



Kanishk Gaur, CEO, India Future Foundation, shared his insights on TikTok and how this platform is facing allegations in the European Market on Mirror Now.

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