INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

NEWS FROM AROUND THE WORLD

MASSIVE DATA BREACH EXPOSES PRIVATE INFORMATION OF CO-WIN APP USERS

In a major data breach, private information of thousands of citizens who registered on the Co-WIN application for the COVID-19 vaccination has been leaked to unauthorized entities. A Telegram bot had been distributing the personal details of individuals, including name, date of birth, phone number and additional information provided during registration, such as passport or Aadhaar number. The breached data also includes details of prominent Indian political leaders.

The Telegram bot initially revealed complete Aadhaar number but later only displayed the last four digits. As a result, those with access to individuals' phone numbers could retrieve details like the particular individual's name, gender, passport number or Aadhaar number and location of the first dose of the COVID-19 vaccine.

Mr Rajeev Chandrasekhar, Union Minister of State for Electronics & Technology did acknowledge that a Telegram bot was retrieving personal details from the Co-WIN app. However, he stated that the data being accessed seemed to originate from a previously breached/stolen database and did not indicate a direct breach of the Co-WIN application.

IN THIS NEWSLETTER

NATIONAL CYBER SECURITY COORDINATOR PROPOSES "DELHI DECLARATION" FOR G20 NATIONS

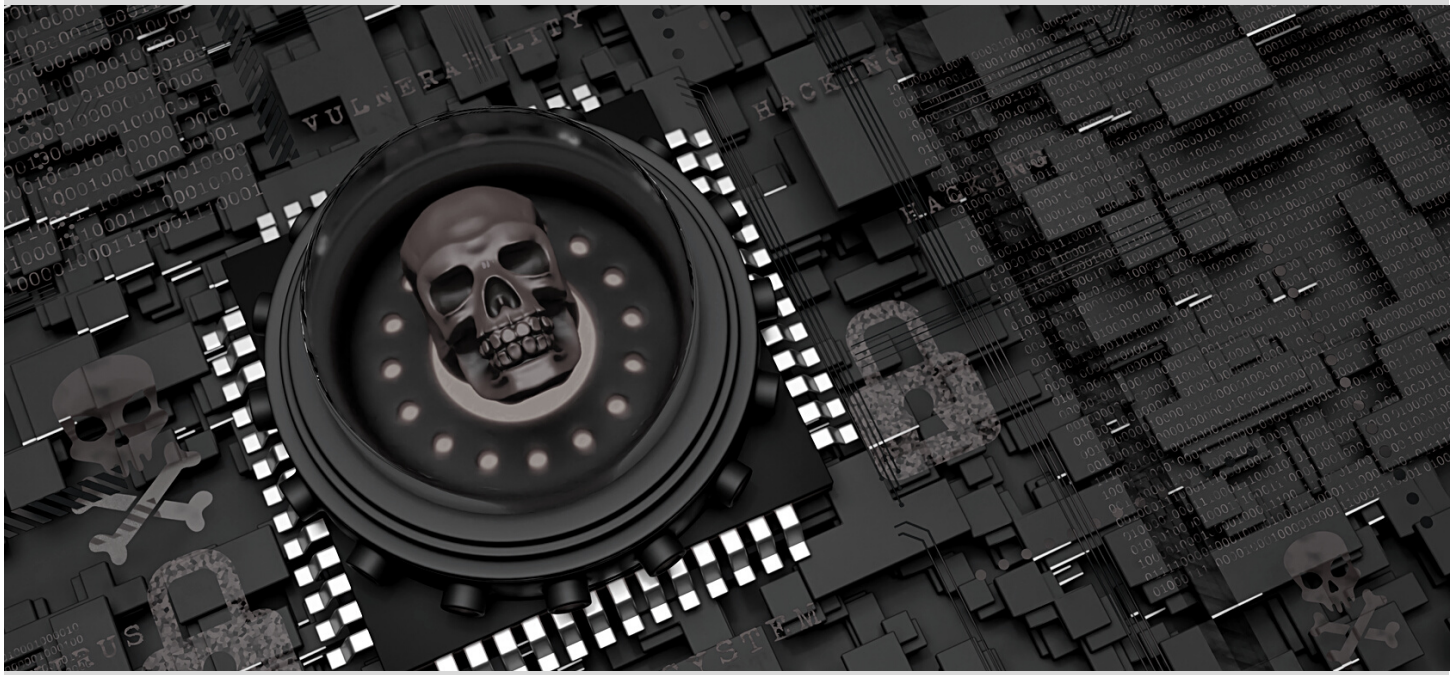
During the B20 India 2023 Conference (the official G20 dialogue forum with the global business community) on cybersecurity organized by the Confederation of Indian Industry (CII), Lt Gen. (Retd) Dr Rajesh Pant, the then National Cyber Security Coordinator, National Security Council Secretariat, Government of India, put forward the "Delhi Declaration" on 05 June 2023, urging G20 nations to collaborate in promoting cyber peace and addressing cyber incidents. Lt Gen. (Retd) Dr Rajesh Pant referred to the existing G20 action plans and laid stress on the support for establishing UN cybersecurity norms.

He highlighted the G20's encouragement for states to adopt responsible state behaviour norms in cyberspace and stated that the Delhi Declaration comprises norms that have already been accepted by the UN and the open-ended working groups. Lt Gen. (Retd) Dr Rajesh Pant shared excerpts from the proposed declaration, expressing the commitment to protect critical infrastructure and peaceful systems from cyber-related harm. He also emphasized the need to cooperate in preventing, mitigating and investigating cyber incidents, particularly ransomware attacks. He outlined additional elements of the Delhi Declaration, including the commitment to safeguard the software supply chain, uphold international law and the rule of law in cyberspace and protect the humanitarian sector. He further emphasized the importance of long-term plans to support the implementation of the framework.

Lt Gen. (Retd) Dr Pant underscored the significance of governance structures and cybersecurity training to ensure cyber hygiene, including the establishment of standard operating procedures, cyber crisis management plans and audits. He highlighted the comprehensive nature of technology within the concept of a zero-trust architecture, encompassing endpoint security, identity and access management, network security, data security, cloud security and application security.

The Delhi Declaration aims to strengthen global cybersecurity cooperation and promote responsible state behaviour in cyberspace. It prioritizes the protection of critical infrastructure, collaborative efforts to prevent cyber incidents, adherence to international law and the enhancement of cybersecurity in the humanitarian sector. The proposed declaration will undergo further deliberation and consideration by G20 nations as part of their joint commitment to address cyber threats and foster cyber peace.

AIIMS DELHI THWARTS MALWARE ATTACK WITH ADVANCED FIREWALL SECURITY SYSTEM



In a significant development, the prestigious All India Institute of Medical Sciences (AIIMS), New Delhi successfully prevented a malware attack on its servers on 06 June 2023, with the help of the implementation of an advanced firewall security system. This accomplishment comes six months after AIIMS, New Delhi suffered a crippling ransomware attack that paralyzed its servers. The institution has since made major structural changes to enhance its cybersecurity measures.

The cyber cell of AIIMS, now under the control of the Defence Research and Development Organisation (DRDO), is working in conjunction with agencies such as the National Critical Information Infrastructure Protection Centre (NCIIPC) and the Indian Computer Emergency Response Team (CERT-In) to investigate the recent attack.

Although the server was temporarily down for approximately four hours due to the firewall trigger, it was a necessary precautionary measure. The cyber cell of AIIMS, New Delhi emphasized that this downtime was a normal occurrence during firewall activities and was in response to the detection of a potential virus. To ensure comprehensive protection in the future, additional security measures would be implemented over the next six months. The proactive stance of the cyber security team at AIIMS, New Delhi was pivotal in detecting and neutralizing the recent malware attack, as reported in an official statement.

The ransomware attack suffered by AIIMS, New Delhi, in November 2022, for over 15 days, severely disrupted online services at the country's premier medical institution. During that incident, at least five servers were compromised. Subsequently, AIIMS, New Delhi made a commitment to fortify its e-hospital network by establishing a dedicated and secure LAN/intranet network managed by its computer facility department.

GLOBAL CYBERATTACK TARGETS US FEDERAL AGENCIES AND NATO ALLIES

In an alarming development, senior government officials of the United States of America (USA) are scrambling to mitigate the impact of a widespread cyberattack that has affected several US federal agencies and allied countries, including members of the North Atlantic Treaty Organization (NATO). The Cybersecurity and Infrastructure Security Agency (CISA) confirmed on 15 June 2023 that it was providing support to affected agencies grappling with intrusions in their file transfer applications.

Ms Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology, National Security Council, USA revealed that the hackers exploited a vulnerability in a commonly used software utilized by companies worldwide for large file transfers. According to cybersecurity experts, this breach is being characterized as one of the most significant theft and extortion events in recent history. Among the victims of the cyberattack are renowned institutions such as Johns Hopkins University, the University of Georgia, the British Broadcasting Corporation (BBC) and British Airways.

According to media reports, the hacking group responsible for the attack has been operational since 2014 and operates from Russia, with the approval of Moscow's intelligence services. Ms Jen Easterly, Director, CISA identified the hacking group as CLOP Ransomware. Mr Brett Callow, Cyber Threat Analyst, Emsisoft revealed that there have been 47 confirmed victims so far, including unidentified US government agencies. CLOP claimed to have impacted hundreds of organizations.

However, no federal agencies have received extortion demands so far, and no federal data has been leaked. According to CISA, many organizations had already patched the vulnerability before the cybercriminals could infiltrate their systems.

GOVERNMENT OF INDIA UNVEILS NATIONAL CYBER SECURITY REFERENCE FRAMEWORK

The Government of India has taken a significant step in countering the increasing incidents of malware attacks on critical sectors by introducing a new policy on cyber security. Lt Gen. (Retd) Dr Rajesh Pant, the then National Cyber Security Coordinator, National Security Council Secretariat, Government of India, announced on 12 June 2023 that the National Cyber Security Reference Framework (NCRF) 2023 has been approved and will soon be made available to the public. He further stated that the policy aims to provide strategic guidance to critical sectors such as banking, energy, and others so that they are empowered enough to tackle cybersecurity concerns effectively.

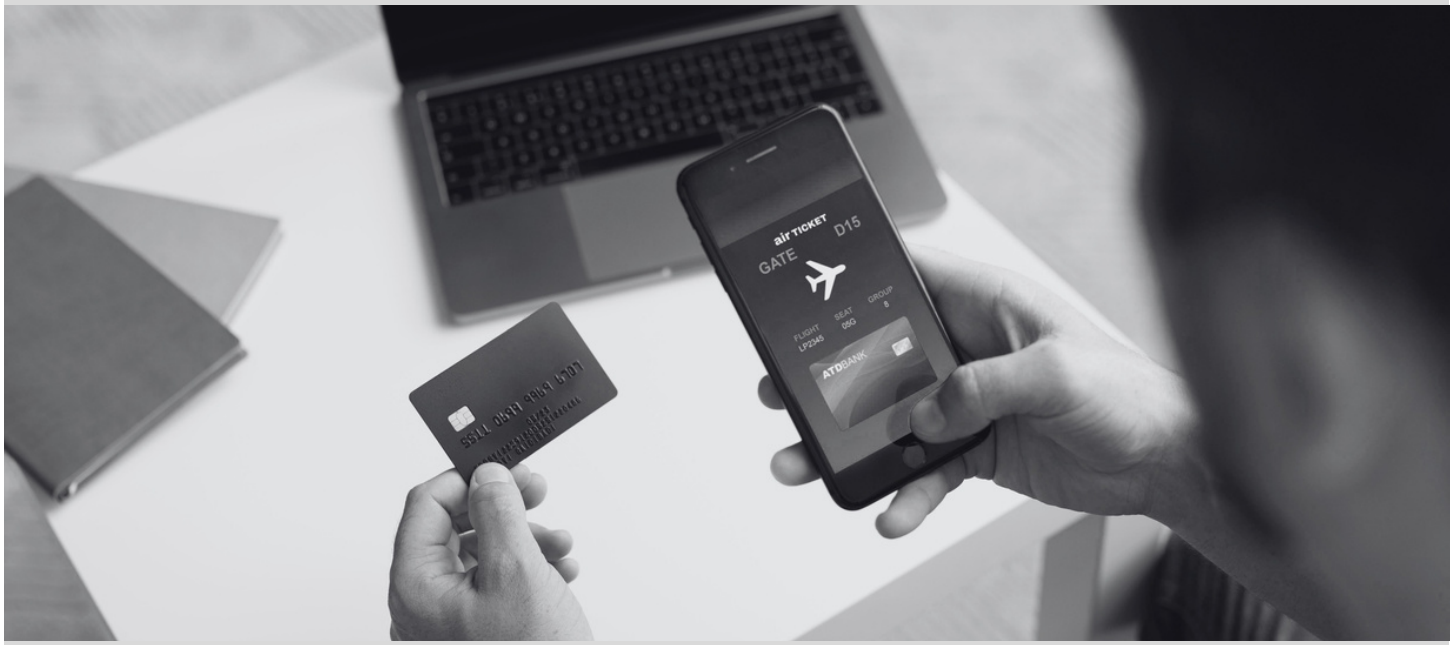
Till date, the government has identified seven sectors as critical. These include telecom, power and energy, banking and financial services, transport, strategic and public enterprises, government, and healthcare. The NCRF has been designed to offer a structured approach to organizations to address their cyber security concerns strategically.

During the India Digital Summit 2023 held on 20 February, 2023 Lt Gen. (Retd) Dr Rajesh Pant had mentioned that the framework, formerly known as the National Cyber Security Strategy 2023, would be released soon. He had also highlighted that the policy would be based on the principle of Common But Differentiated Responsibility (CBDR).

Industry experts have emphasized that the NCRF 2023 represents the first update to the Ministry of Electronics and Information Technology's (MeitYs) National Cyber Security Policy 2013, which aimed to provide enterprises with guidelines on best practices to prevent cyberattacks. The policy would differ from directives issued by Cert-In on 28 April, 2023. The Cert-In regulations established a six-hour timeline for companies to report cyber incidents, failure of which could result in penalties under Section 70B of the Information Technology Act, 2000.

However, experts have expressed concerns regarding the framework document, suggesting that it may not have any legal implications to enhance India's cyber security environment. They further stressed the importance of dedicated regulations focused on cyber security, especially in light of recent incidents such as the cyberattack on the All India Institute of Medical Sciences (AIIMS), New Delhi in November 2022 and the reported data breach on the government's COVID-19 vaccination platform, Co-WIN.

RESERVE BANK OF INDIA INTRODUCES DRAFT REGULATIONS TO STRENGTHEN CYBER SECURITY



To address the emerging cyber risks associated with digital payments, the Reserve Bank of India (RBI) announced draft regulations on 02 June 2023 for Payment System Operators (PSOs). The proposed norms aim to enhance the safety and security of digital transactions and are set to be implemented in a phased manner. Under the draft regulations, large non-bank PSOs will be required to comply with the norms starting 01 April 2024. Medium-sized non-bank PSOs have been given a deadline of 01 April 2026 while smaller ones have to comply with these guidelines until 01 April 2028.

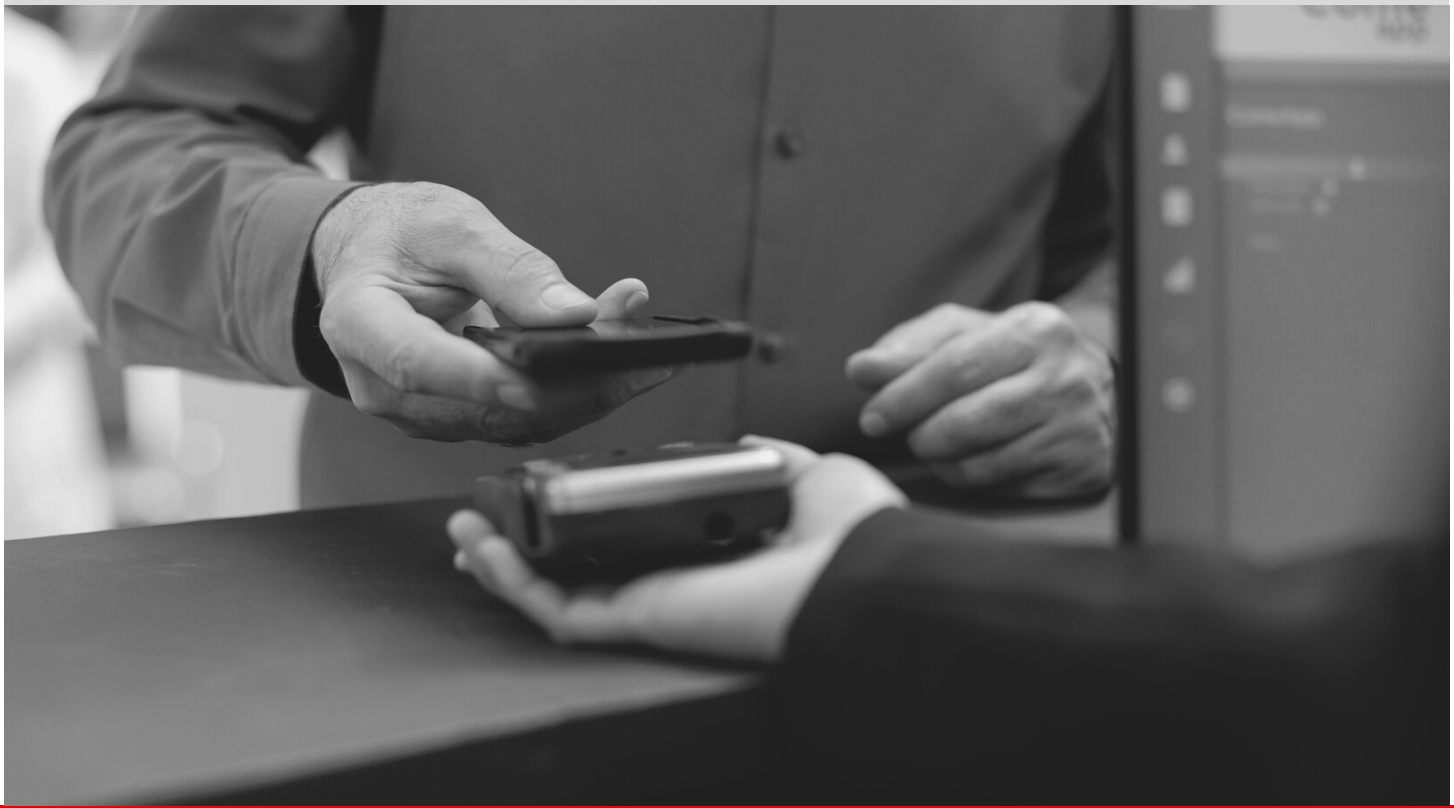
The RBI's draft directions emphasize the need for robust governance mechanisms to identify, assess, monitor and manage cyber security risks. These regulations also aim to establish baseline security measures to ensure the resilience and security of digital payment transactions. While the PSOs are expected to migrate to the latest security standards, the existing instructions on security and risk mitigation measures for card payments, Prepaid Payment Instruments (PPIs) and mobile banking will continue to remain applicable.

According to the draft norms, PSOs will be required to define appropriate Key Risk Indicators (KRIs) to identify potential risk events and Key Performance Indicators (KPIs) to assess the effectiveness of security controls. The board of the PSOs will be responsible for ensuring adequate oversight over information security risk, with the possibility of delegating primary oversight to a board sub-committee that meets quarterly. To ensure cyber resilience, the PSOs will be required to conduct cyber-risk assessment exercises when launching new products, services technologies, or implementing significant changes to existing infrastructure or processes. The Chief Information Security Officer (CISO) or an equivalent executive will oversee the implementation of action points arising from such assessments.

The proposed regulations also call for the formulation of an Information Security (IS) policy approved by the PSO's board, covering potential information security risks across all payment system applications and products. Additionally, PSOs will need to develop a Business Continuity Plan (BCP) based on various cyber threat scenarios, including extreme but plausible events. The BCP should be reviewed at least once a year and include a comprehensive cyber incident response, resumption and recovery plan to effectively manage cyber security events.

The draft norms emphasize the importance of a separate board-approved Cyber Crisis Management Plan (CCMP) to detect, contain, respond to and recover from cyber threats and attacks. To ensure the implementation and continuous assessment of information security and cyber resilience, a senior-level executive, such as the CISO, should be entrusted with responsibility and accountability.

Further, the PSOs are required to implement measures to protect their networks and systems from external threats. They must also establish a comprehensive data leak prevention policy to safeguard the confidentiality, integrity, availability and protection of business and customer information, both in transit and at rest.



CANADA TO LAUNCH CYBER SECURITY CERTIFICATION PROGRAMME

In a bid to fortify cyber security measures and safeguard Canada's defence industry from cyber threats, the Government of Canada has unveiled plans to establish the Canadian Programme for Cyber Security Certification (CPCSC). The programme is expected to introduce mandatory certification requirements for select federal defence contracts by winter of 2024. The CPCSC aims to enhance the resilience of critical supply chains and protect national security and to create more international procurement opportunities for Canadian suppliers.

The Honourable Ms Anita Indira Anand, Minister of National Defence, announced the government's commitment to developing and implementing the cyber security certification programme on behalf of the Honourable Ms Helena Jaczek, Minister of Public Services and Procurement. Through collaboration with Public Services and Procurement, Canada, the Department of National Defence and the Standards Council of Canada, the government plans to engage with the defence industry and key stakeholders through upcoming sessions in late 2023 to shape the programme's development.

The CPCSC aims to establish mutual recognition between Canada and the United States. This recognition would enable certified Canadian suppliers to be acknowledged in both jurisdictions, thereby building trust in the resiliency of Canadian suppliers and unlocking procurement opportunities with close allies.

The Honourable Mr François-Philippe Champagne, Minister of Innovation, Science, and Industry, stressed on the significance of the certification programme in protecting critical supply chains and ensuring Canadian suppliers' participation in US defence procurement. He further emphasized that the programme is critical for industry growth, job creation, and prosperity across Canada.

KASPERSKY AND IIT BOMBAY COLLABORATE

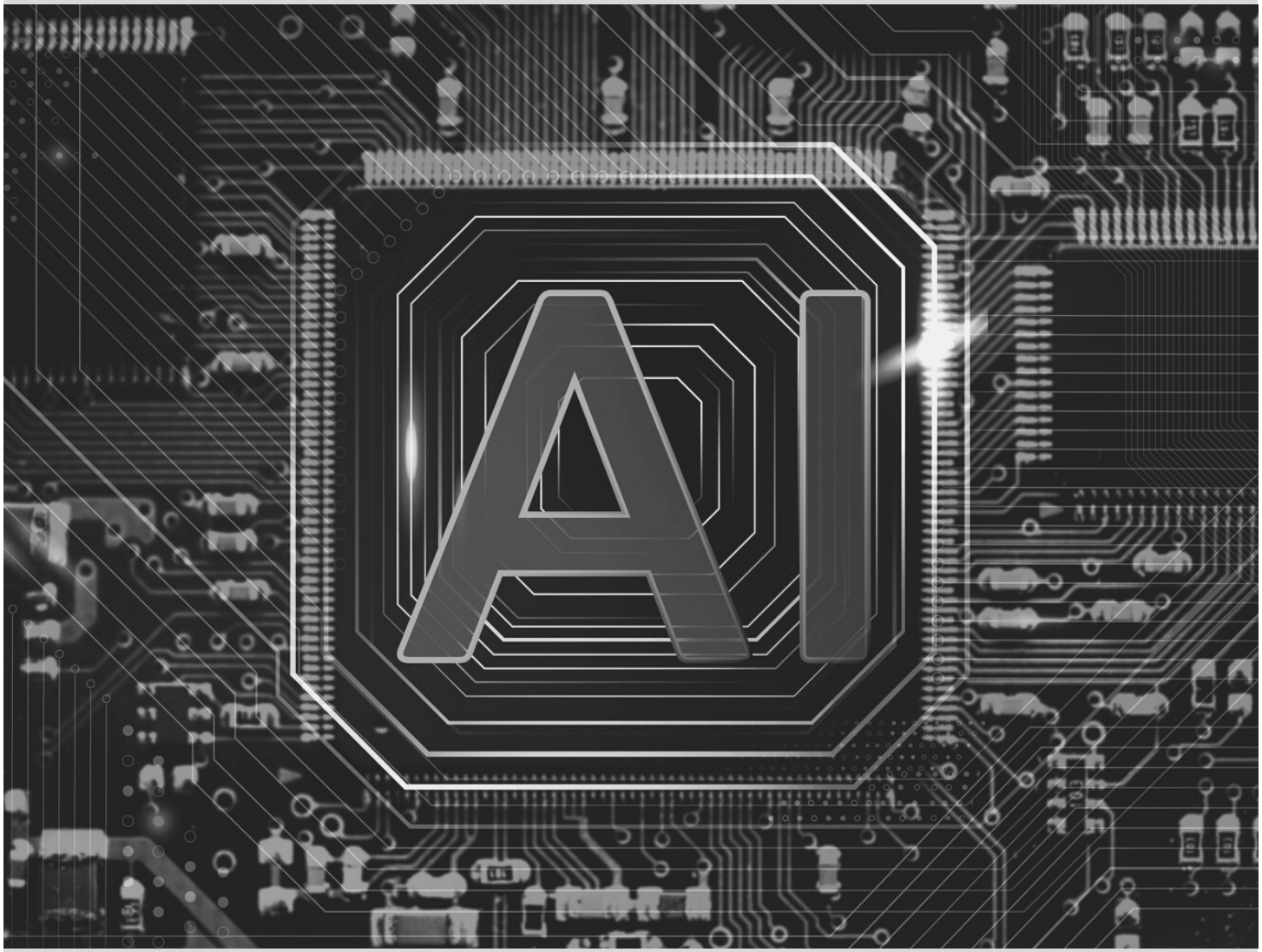
Global cybersecurity company, Kaspersky, and the prestigious Indian Institute of Technology (IIT), Bombay have signed a Memorandum of Understanding (MoU) to jointly promote and foster development of educational and research projects in the field of cybersecurity. The agreement solidifies the partnership between Kaspersky and IIT Bombay to advance cybersecurity education and research, with the aim of cultivating a stronger cybersecurity workforce, in India. The collaboration underscores the commitment of both parties for closer cooperation in enhancing the security of the computing environment. Some of the key areas of collaboration include exchange of knowledge and expertise, development of educational materials, organization of cybersecurity awareness events, and sponsorship of awards and book prizes to inspire students to pursue careers in cybersecurity.

UK AND SINGAPORE HOLD DIALOGUE TO STRENGTHEN CYBERSECURITY COOPERATION

The Cyber Security Agency of Singapore (CSA) and the United Kingdom's (UK) Foreign, Commonwealth and Development Office (FCDO) held a dialogue to enhance cybersecurity cooperation between the two countries. The dialogue was co-chaired by Mr David Koh, Chief Executive, Singapore's Cyber Security Agency and Mr Will Middleton, Cyber Director, FCDO. The dialogue, attended by senior officials from both countries, aimed to strengthen the already close ties in cyber cooperation. It builds upon the UK-Singapore Cybersecurity Memorandum of Understanding (MoU), a result of the UK-Singapore Digital Economy Agreement.

During the dialogue, both sides explored opportunities for deeper cooperation in areas such as Internet of Things (IoT) security, app security, and cyber skills development. They emphasized the importance of securing apps and app stores, expressing a desire to explore the potential for an international standard. Recognized international standards and norms for IoT were also highlighted and plans were made to work together on mutual recognition of IoT schemes and collaboration in other IoT domains. Further, efforts to map the skills and competencies of cybersecurity professionals in Singapore and the UK were also discussed.

EUROPEAN UNION PARLIAMENT APPROVES AI RULES



In a significant milestone, the European Union (EU) Parliament has given its approval to the EU AI Act, a set of groundbreaking regulations governing AI. This momentous decision marks the first formal regulation of AI in the Western world and sets the stage for its eventual adoption into a law. As part of the EU AI Act, the European Parliament has chosen to impose stricter regulations on generative AI tools such as ChatGPT. Developers of generative AI systems will be required to undergo a review process before commercial release.

Further, the Parliament has maintained its stance on banning real-time biometric identification systems and controversial "social scoring" systems, despite attempts by some to dilute the prohibition. Lawmakers have remained firm in their decision and agreed to prohibit biometric surveillance in all public settings. These laws will have far-reaching implications for developers of generative AI models, including Microsoft-backed OpenAI's ChatGPT and Google's Bard. The next stage involves negotiators from EU institutions, including the executive body and the 27 member states, coming together to refine and finalize the regulations.

NATIONAL INTERNET SAFETY MONTH

Every June, National Internet Safety Month takes centre stage as an annual initiative dedicated to raising awareness and educating individuals on the importance of online safety. With the participation of federal and state governments, industry leaders, and nonprofit organizations, this month-long campaign aims to promote responsible and secure online behaviour. The key emphasis of this initiative is the notion of unity, recognizing that ensuring Internet safety is a collective responsibility that requires the collaboration of individuals, communities and organizations.

Throughout the entire month of June, various stakeholders join forces to advocate for safe practices and foster a better understanding of online risks and preventive measures. The objective is to create a safer digital environment for everyone, whether they are navigating the Internet at work or in the comfort of their homes.

National Internet Safety Month serves as a reminder that online safety is not an individual endeavour but a shared commitment. It highlights the need for individuals to come together and actively contribute to making the Internet a secure space for all users. By pooling resources and expertise, stakeholders work collaboratively to address the evolving challenges posed by the digital landscape.

The focus of National Internet Safety Month extends beyond merely raising awareness. It also emphasizes the importance of taking concrete steps to protect oneself and others in the digital realm. This includes adopting strong passwords, regularly updating softwares and applications, exercising caution while sharing personal information online, and being mindful of the consequences of online actions.

CYBER MANTHAN - SECURING INDIA'S ENERGY SECTOR

India Future Foundation (IFF) in collaboration with Microsoft, organized a hybrid consultation under the brand name, Cyber Manthan – Securing India's Energy Sector. The event was organized on 01 June 2023 at The Oberoi, New Delhi. Some of the focus areas on which the speakers at the consultation deliberated were global trends in the energy sector, the sophisticated nature of cyberattacks, existing vulnerabilities and solutions that can be employed, by the sector to alleviate the risks posed by cyberattacks. Through this Cyber Manthan, we aimed at highlighting the need for establishing cyber security guidelines and regulations to safeguard India's energy sector from cyberattacks.

The speakers at the consultation included Lt Gen. (Retd) Vinod G. Khandare, Principal Advisor, Ministry of Defence, Government of India; Maj. Gen. Manjeet Singh, Joint Secretary (Cyber), National Security Council Secretariat, Government of India; Maj. Gen. (Retd) Dr Pawan Anand, Distinguished Fellow & Head USI-ANBI, The United Service Institution of India; Maj. Gen. (Retd) PK Mallick, Defence and Cybersecurity Expert; Mr Jean-Philippe Courtois, Executive Vice President & President, National Transformation Partnerships, Microsoft; Mr Rakesh Maheshwari, Former Senior Director & Group Coordinator-Cyber Law and Data Governance, Ministry of Electronics and Information Technology (MeitY), Government of India; Col (Retd) Sanjeev Relia, Chief Strategy Officer, ThinkCyber India; Dr Subi Chaturvedi, Chief Corporate Affairs & Public Policy Affairs Officer, InMobi; Dr Charru Malhotra, Professor (e-Governance and ICT), Indian Institute of Public Administration; Ms Irina Ghose, the then Chief Operating Officer, Microsoft India; Dr Rohini Srivathsa, National Technology Officer (CTO), Microsoft India; Mr Terence Gomes, the then Country Head Security, Microsoft India; Mr Sandeep Aurora, Director - Government Affairs &Public Policy Microsoft; Mr Aamod Omprakash, Cyber and Digital Policy Officer, Embassy of The United States of America, New Delhi and Mr Dominic Gillan, First Secretary - Cyber Programmes, British High Commission, New Delhi.

CONSULTATION ON EMERGING THREAT LANDSCAPE

India Future Foundation (IFF) in collaboration with Microsoft organized a virtual consultation on "The Emerging Threat Landscape" on 23 June 2023. The discussion revolved around emerging threats and vulnerabilities impacting India, importance of adopting a cyber resilience strategy, People Process Technology (PPT) Model, how can CISOs make a start on Zero Trust and the need for Cloud Security Regulation.

With the rising popularity of technologies like Metaverse, new threats are introduced. Additionally, while artificial intelligence (AI) and machine learning (ML) offer immense benefits in areas such as research and analytics, they also present new opportunities for advanced attacks when wielded by malicious actors. The deployment of deep fakes and the proliferation of bots further complicate the threat landscape.

Among the most concerning threats are Advanced Persistent Threat (APT) attacks, which are sophisticated and stealthy campaigns carried out by well-resourced adversaries. These attacks involve prolonged infiltration into targeted networks, aiming to gather sensitive information or disrupt critical infrastructure. Another pervasive threat is ransomware attacks, where malicious actors encrypt valuable data and demand ransom payments for its release. These attacks have witnessed a surge in frequency and sophistication, often targeting organizations of all sizes, from individuals to large corporations. Additionally, third-party supply chain attacks have become a growing concern, exploiting vulnerabilities in the inter-connected ecosystem of software and hardware providers. By compromising a trusted third party, threat actors can gain unauthorized access to multiple organizations, amplifying the impact of their attacks.

The aim of the consultation was to gain a comprehensive understanding of the current and evolving threats faced by individuals, organizations and society as a whole. The consultation aimed to identify and analyze the emerging trends, vulnerabilities and potential risks associated with various domains. Further, the discussion also revolved around how to mitigate risks, strengthen resilience and foster a safer and more secure environment in the face of emerging threats.

The speakers at the consultation included Mr Rakesh Maheshwari, Former Senior Director & Group Coordinator-Cyber Law and Data Governance, Ministry of Electronics and Information Technology (MeitY), Government of India; Ms Smita Jain, Senior Cyber Security Technology Specialist, Microsoft; Dr Pavan Duggal, Advocate, Supreme Court of India; Mr Manzar Abbas, Chief Information officer, AVP IT, Orient Electric; Dr Shruti Mantri, Associate Director, Indian School of Business; Mr Pranav Mishra, Head - Govt Affairs and Policy, AMD; Mr Aamod Omprakash, Cyber and Digital Policy Officer, Embassy of the United States of America, New Delhi; Mr Kanishk Gaur, Founder, India Future Foundation; Mr Pankaj Anup Toppo, Head - Policy Programmes & Research, India Future Foundation and Ms Manmeet Randhawa, Head - Corporate Communications & Strategic Alliances, India Future Foundation.

PANEL DISCUSSION ON BECOMING CYBER RESILIENT: UNDERSTANDING CFO'S STRATEGIES, INVESTMENTS AND DECISION MAKING

IMA in collaboration with Microsoft, organised a panel discussion with Chief Financial Officers (CFOs) of Indian and Foreign MNCs across various sectors to understand and explore issues around the CFO's role in Cybersecurity. Cybersecurity has become a critical concern for organizations worldwide as they navigate the increasingly complex digital landscape. With cyber threats evolving and becoming more sophisticated, it is imperative for businesses to enhance their cyber resilience.

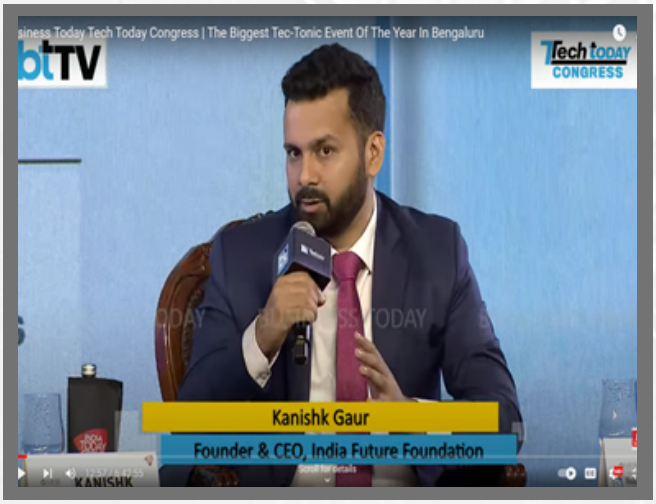
Mr Amit Dubey, Co–Founder, India Future Foundation participated in this panel discussion. He emphasized on the necessity of a comprehensive cybersecurity strategy that aligns with organizational objectives and risk tolerance. He further emphasized the integration of cybersecurity into financial planning and decision-making processes, stressing the importance of allocating adequate resources to safeguard critical assets.

The event brought together CFOs from Indian and foreign MNCs representing diverse sectors. The panel discussion served as a platform for CFOs to share their experiences, insights, and strategies for addressing the ever-growing cybersecurity challenges faced by organizations. The event aimed to create awareness about the significant role leaders in the finance sector play in ensuring the safety and security of digital assets and the overall stability of businesses in an increasingly interconnected world.

IFF IN THE MEDIA

Mr Kanishk Gaur, Founder, IFF, shares his opinion on impact of PM Modi's visit on India-US collaborations in *The Financial Express*.

Mr Kanishk Gaur, Founder, India Future Foundation provides insights on enterprise cybersecurity in *CIO&LEADER*.



Mr Kanishk Gaur, Founder, IFF, spoke about the drawback of relying too much on AI language models at the *Business Today Tech Today Congress*.

Mr Kanishk Gaur, Founder, IFF, shared his views on Prime Minister Modi's US visit, in *ETGovernment.com*.

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