INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

INDIA INTRODUCES FIRST CYBER QUANTIFIED MODEL FOR RISK MANAGEMENT

In response to the escalating pace of cyber threats and the tightening regulatory landscape, Mumbai-based cybersecurity startup Zeron has unveiled India's maiden advanced Cyber Quantified model— the Quantified Business Exposure to Risks (QBER)— for the BFSI (Banking, Financial Services, and Insurance) sector. As the inaugural CRQ (Cyber Risk Quantification) model from India, QBER heralds a new era in cyber risk assessment, offering organisations a comprehensive and dynamic approach to cybersecurity management.

IN THIS NEWSLETTER

By quantifying cyber risks in monetary terms and providing actionable insights, QBER empowers organisations to bolster their cyber resilience, streamline operations, and effectively mitigate the financial ramifications of cyber incidents. The market demand for CRQ solutions, as exemplified by QBER, is robust and is rapidly expanding. As cyber threats evolve in sophistication and frequency, organisations across industries seek innovative tools to quantify and manage their cyber risk exposure efficiently. Statistics reveal that globally 97 per cent of organisations that adopted CRQ derived significant benefits with regards their investments in cybersecurity.

In contrast to traditional approaches, QBER offers a dynamic and holistic perspective of cyber risk exposure, enabling organisations to adapt swiftly to the evolving threat landscape. By integrating QBER into insurance underwriting processes and credit risk analysis actions, insurers can customise policies to clients' unique risk profiles, fostering a more resilient cybersecurity ecosystem.

This development comes amidst a surge in cyber threats, data breaches, and extortion cases impacting businesses. Zeron aims to leverage advanced threat intelligence to give financial organisations timely insights into their cyber risk exposure. By incorporating industry-specific data such as market capitalisation, employee count, endpoints, security solutions, and regulatory mandates, QBER empowers organisations to make informed decisions regarding cyber risk mitigation strategies, resource allocation, and regulatory compliance.

This launch signifies a pivotal moment in India's cybersecurity landscape, addressing two critical challenges confronting organisations today: the rapidly evolving cyber threat landscape and the tightening regulatory environment. With cyber threats increasing at an unprecedented rate and regulatory requirements imposing greater accountability, the demand for robust cyber risk management solutions has never been more acute.

AMNESTY INTERNATIONAL CITES INDONESIA AS A SPYWARE HUB

Amnesty International's Security Lab research has identified Indonesia as an emerging surveillance tool and supplier hub. The organisation found evidence of sales and shipments of "highly invasive spyware and other surveillance technologies" sent to Indonesia from countries such as Israel, Greece, Singapore, and Malaysia, dating back to 2017 and continuing until last year.

These surveillance tools reportedly come from companies like Q Cyber Technologies (linked to NSO Group), the Intellexa consortium, Saito Tech (also known as Candiru), FinFisher and its wholly-owned subsidiary Raedarius M8 Sdn Bhd, and Wintego Systems.
Amnesty International also detailed various malicious domain names and network infrastructures connected to spyware platforms targeting individuals in Indonesia. While the domain names mimic political parties and media outlets, it is unclear who is being targeted. Historically, spyware has been used by government entities to target civil society and journalists. For Indonesia, where civil rights are under increasing assault, this is particularly concerning, according to the Amnesty's report.

The growing deployment of surveillance technology in Indonesia raises significant concerns about the erosion of citizens' civil rights in the country.

COMPANIES WARY OF AI-FUELLED MALWARE AND PHISHING

A large majority of cybersecurity leaders worldwide are increasingly concerned about the negative impact of AI on cybersecurity, according to a new global survey by CyberArk. The 2024 Identity Security Threat Landscape Report reveals that 93 per cent of respondents anticipate significant negative consequences from AI, particularly from AI-powered malware and phishing attacks.

The Key Findings of the CyberArk Report are as follows:

1. High Concern Over AI Risks: The survey, which included responses from 2,400 cybersecurity leaders across 18 countries, underscores the widespread apprehension about AI's potential to enhance cyber threats. The top concerns include AI-powered malware and sophisticated phishing attacks.

2. Cyber Debt and AI: The report highlights the growing issue of "cyber debt," exacerbated by the rise of Generative AI (GenAI), machine identities, and increasing third- and fourth-party risks.

3. Increased AI Utilization in Defence: About 99 per cent of organisations leverage AI to bolster their cybersecurity defences despite the risks. However, this double-edged sword also increases the sophistication and volume of identity-related attacks.

4. Phishing and Vishing Attacks: In the past year, 90 per cent of organisations experienced breaches due to phishing or vishing attacks. These attacks will become more challenging to detect as AI automates and personalises them.

5. Indian Organizations and Identity Breaches: In India, 93 per cent of organisations reported experiencing two or more identity-related breaches in 2023, indicating an exceptionally high vulnerability in this region.

6. Deepfakes and Election Interference: The report raises alarms about the potential for AI-powered deepfake campaigns to influence election outcomes, with over 4 billion voters in more than 60 countries preparing for elections in 2024.

7. Machine Identities at Risk: Machine identities are identified as a significant source of risk. Bad actors could exploit these identities using AI to execute large-scale attacks.

The implications and recommendations suggested in the report, to mitigate the impact of the risks as highlighted in the report are mentioned below.

1. Enhanced Vigilance: Organizations must remain vigilant and adapt their cybersecurity strategies to counter the evolving AI-driven threats.

2. AI in Cyber Defence: While AI is a powerful tool for enhancing cybersecurity, it also requires robust monitoring and management to prevent its misuse by malicious actors.

3. Comprehensive Training: Cybersecurity teams need continuous training to stay ahead of AI-powered threats and improve their ability to detect and mitigate sophisticated attacks.

4. Collaboration and Sharing: Global collaboration and threat intelligence sharing can help organisations better prepare for and respond to AI-driven cyber threats.

LESSONS FROM LATIN AMERICA'S BATTLE AGAINST RANSOMWARE THREATS

Latin American countries are increasingly focusing on enhancing their cyber resilience in response to a spate of ransomware attacks. The "Cyber Readiness in Latin American Public Sectors: Lessons from the Frontline" report, produced by the Digi Americas Alliance, a multistakeholder and interdisciplinary network of organisations from diverse sectors interested in cyber and digital issues based in Washington, United States and its LATAM CISO Network in collaboration with Duke University, Durham, North Carolina, United States outlines the advanced cyber measures adopted across the region.

Key Insights from the Report

Robust Cybersecurity Policies: Countries like Costa Rica and Colombia have established comprehensive cybersecurity policies following significant cyber incidents, in their respective countries. This proactive approach aims to improve defences and protect critical infrastructure.

Adoption of Risk Management Frameworks (RMFs): The report highlights the growing adoption of RMFs across Latin America. About 94 per cent of survey respondents believe that implementing RMFs can enhance organisational resilience against cyber threats like ransomware. Approximately 72 per cent have already integrated RMFs into their cybersecurity strategies.

Cloud Solutions for Enhanced Security: With the need for more robust data security, cloud-based services are increasingly adopted. According to the survey, 78 per cent of respondents are using or planning to implement cloud-based cybersecurity infrastructure.

Reactive and Proactive Measures: The report notes a trend towards reactive strengthening of defences post-attack. For instance, Costa Rica declared a state of emergency and developed a new national cyber strategy following an attack. Colombia introduced legislative bills to create a specialised digital security authority.

International Collaboration: International partnerships are playing a crucial role in enhancing cybersecurity. Costa Rica, for instance, has signed memorandums of understanding with Israel, Japan, and the United States of America. The USA has committed $25 million to help establish a cybersecurity operations centre in Costa Rica by 2026.

Human Capital Development: A significant focus is on workforce development and education. The report emphasises on the need for expanded cybersecurity training programmes and increased cyber awareness. Investing in human capital is essential for developing a mature and resilient cybersecurity culture.

Recommendations for Strengthening Cybersecurity

Invest in Human Capital: Developing a skilled workforce through comprehensive training programs and educational initiatives is critical. This investment will enhance cyber resilience and foster a robust cybersecurity culture.

Establish a Voluntary RMF: Creating a voluntary RMF with mixed governance, a national cybersecurity incident response team (CSIRT), and sector-specific incident databases can improve coordination and response effectiveness.

Invest in Cybersecurity Infrastructure: Continuous investment in modern cybersecurity infrastructure and technologies, including cloud solutions and security software, is essential to defend against emerging threats.

Centralise Cybersecurity Management: Implementing centralised cybersecurity management and reporting systems ensures rapid, coordinated responses to cyber incidents. This approach enables quicker detection, assessment, and resolution of threats.

MICROSOFT CEO SATYA NADELLA'S MEMO ON PRIORITIZING SECURITY

Mr Satya Nadella, CEO, Microsoft recently addressed Microsoft's employees about prioritising security in the company's operations. He highlighted that Microsoft's success is fundamentally built on trust, and maintaining this trust is essential. Nadella pointed to the recent findings by the Department of Homeland Security's Cyber Safety Review Board regarding the Storm-0558 cyberattack as evidence of the severe threats faced by the company and its customers.

He mentioned the launch of the Secure Future Initiative (SFI) in November 2023, which aims to advance cybersecurity protection across new products and legacy infrastructure. Nadella expressed pride in the initiative but emphasised on the need for further commitment and action. Going forward, Microsoft will dedicate the entire organisation to SFI, guided by three core principles: **Secure by Design, Secure by Default, and Secure Operations.**

These principles will be integral to various aspects of SFI, including protecting identities and secrets, isolating production systems, safeguarding networks, securing engineering systems, monitoring and detecting threats and accelerating response and remediation efforts. Nadella explained that specific, company-wide actions have been outlined for each pillar, including recommendations from the Cyber Safety Review Board (CSRB) report. He noted that implementing these standards and guidelines will be critical in hiring and reward decisions, with senior leadership compensation tied to progress on security milestones.

Nadella stressed on the importance of approaching the challenge with technical and operational rigour, focusing on continuous improvement. He emphasised that every task, from coding to customer interactions, is an opportunity to enhance security. Learning from adversaries and leveraging the vast array of signals Microsoft monitors will be crucial in strengthening the company's security posture. He also highlighted the need for more collaboration between the public and private sectors.

Nadella concluded that security is a collective responsibility and should be the top priority for everyone at Microsoft. He instructed employees to prioritise security over other tasks, including releasing new features or supporting legacy systems, to protect customers' digital estates and build a safer digital environment for all.

CYBER ATTACKS SURGE GLOBALLY IN Q1 2024

Cyberattacks have escalated significantly in the first quarter of 2024, with India being one of the most targeted nations. According to a recent report by Check Point Software Technologies Ltd., there was a 28 per cent increase in global cyberattacks compared to the previous quarter. India faced an average of 2,807 weekly attacks, marking a 33 per cent year-on-year increase, highlighting its position as a prime target for cybercriminals.

The report identified the Education/Research, Government/Military, and Healthcare sectors as the most heavily attacked. Notably, the Hardware Vendor industry experienced a substantial 37 per cent rise in cyberattacks year-on-year, indicating a shift in the focus of cybercriminals.

Regionally, Africa saw a 20 per cent increase in attacks per organisation, while Latin America experienced a 20 per cent decline. North America was the most affected by ransomware attacks, accounting for 59 per cent of the nearly 1,000 reported incidents. Europe followed with 24 per cent and Asia-Pacific with 12 per cent. Europe witnessed the largest increase in ransomware attacks, with a significant 64 per cent rise, in attacks, compared to Q1 2023.

In India, the top malware included FakeUpdates (a botnet and downloader), remote access trojans (RATs), botnets, and information stealers. Over half of the malicious files in India were delivered via the web in the last 30 days. The most common vulnerability exploit type was Remote Code Execution, affecting 64 per cent of organisations in the country.

To combat these escalating threats, experts at Check Point recommend businesses adopt multi-faceted cybersecurity strategies. These include robust data backups, frequent cyber awareness training, timely security patches, strong user authentication, and advanced anti-ransomware solutions.

CHINESE STATE-ALIGNED THREAT GROUP TARGETS GOVERNMENTS GLOBALLY

A recent report by Palo Alto Networks' Unit 42 uncovered a sophisticated espionage campaign orchestrated by a Chinese state-aligned threat group, Operation Diplomatic Specter. This operation, active since late 2022, has been targeting high-level government and military entities across the Middle East, Africa and Southeast Asia.

Operation Details

Operation Diplomatic Specter aims to extract classified and sensitive information about geopolitical conflicts, diplomatic missions, military operations, and political meetings.

To gain initial access, the threat group exploits vulnerabilities in Web and Microsoft Exchange servers, such as ProxyLogon and ProxyShell. They utilise various malicious tools, including open-source programmes and custom backdoors like SweetSpecter and TunnelSpecter.

The campaign focuses on ministries of foreign affairs, military entities, embassies and more across at least seven countries on the three continents.

Tools and Techniques

- The attackers employ various techniques, including keyword searches, to filter information relevant to the People's Republic of China, such as military data and material related to political leaders.
- They use well-known Chinese malware families like PlugX and China Chopper and custom backdoors like SweetSpecter and TunnelSpecter.

Defence Strategies

- Organisations are advised to prioritise patching and hardening Internet-facing assets to prevent initial access.
- Implementing layered security measures, including network monitoring, detection and response, and cloud email solutions, is crucial to mitigating the risk posed by sophisticated threat actors like Diplomatic Specter.

LOCKBIT RINGLEADER IDENTIFIED, SANCTIONS IMPOSED

Law enforcement agencies in Australia, Europe, and the US have identified and unmasked the mastermind behind the notorious ransomware gang, LockBitSupp. Dmitry Yuryevich Khoroshev, a Russian national, is revealed to be the orchestrator of the cybercrime group responsible for substantial financial losses and widespread ransomware attacks.

Dmitry Yuryevich Khoroshev, aged 31, is identified as the leader of LockBitSupp, a group responsible for significant ransomware attacks globally. The gang reportedly amassed over $100 million through its criminal activities.

Australian businesses and individuals now face government sanctions for engaging with LockBitSupp or paying ransoms. Penalties include fines for companies and criminal charges for individuals providing assets to Khoroshev.

The identification of Khoroshev follows the collaborative efforts of law enforcement agencies worldwide under Operation Cronos. This operation led to dismantling of LockBitSupp's infrastructure and subsequent arrests, cryptocurrency seizures and sanctions.

Australia's foreign affairs minister, Penny Wong, emphasised on the country's commitment to upholding cybersecurity norms and holding cybercriminals accountable through sanctions. The move aims to disrupt the ransomware business model and prevent further attacks on Australian citizens and businesses.

CHINESE ORB NETWORKS TRANSFORM CYBER-ESPIONAGE LANDSCAPE

Mandiant, an American Cybersecurity firm, has uncovered a sophisticated evolution in Chinese cyber-espionage tactics. Dubbed the Operational Relay Box (ORB) network, this clandestine infrastructure represents a paradigm shift in how threat actors conceal their malicious activities.

Mandiant's analysis exposes the intricate structure of ORB networks, comprising virtual private servers (VPS) and compromised smart devices and routers. These networks serve as covert relay stations, enabling Chinese threat actors to orchestrate cyber-espionage operations with unprecedented stealth.

Chinese threat actors leverage ORBs to obfuscate their activities, rendering traditional static indicators of compromise (IoCs) obsolete. The temporary nature of ORB nodes and their extensive global reach present formidable challenges for defenders attempting to attribute attacks.

ORBs encompass provisioned and non-provisioned nodes, spanning diverse geographic locations and hardware types. This hybrid approach enhances resilience and evades detection, allowing threat actors to operate effectively.

With the rise of ORB networks, cybersecurity defenders must adopt a proactive, behaviour-based approach to threat detection. Instead of relying on IP blocking, organisations must analyse infrastructure patterns and SSL/SSH certificates to identify malicious activities.

The emergence of ORB networks underscores the urgency for a paradigm shift in cybersecurity practices. By treating ORBs as dynamic entities, defenders can effectively develop more adaptable defence strategies to counter evolving cyber threats.

EXPLORING INTERPOL'S CYBERCRIME COMBAT STRATEGY: 6 KEY INSIGHTS

As cybercrime continues to increase globally, the International Criminal Police Organization (Interpol) stands at the forefront of the battle against digital threats.

Here are six crucial facts shedding light on how Interpol orchestrates its relentless fight against cybercriminals:

1. Four Global Programmes: Interpol's cybercrime endeavours constitute one of its four primary global programmes, alongside terrorism, organised crime, financial crime and corruption. This underscores the organisation's multifaceted approach to combating digital threats worldwide.

2. Facilitator, Not Executor: Unlike popular belief, Interpol does not directly lead cybercrime investigations or make arrests. Instead, it serves as a programme management agency, fostering collaboration among law enforcement agencies across 196 member countries.

3. Global Coordination: With a politically neutral stance, Interpol operates through a constitutional framework, ensuring governance by its member countries. It acts as a neutral mediator, facilitating collaboration among nations with varying cybercrime-fighting capabilities.

4. Three Core Components: Interpol's cybercrime programme comprises three major components: Cybercrime Threat Response, Cyber Strategy and Capabilities Development, and Cybercrime Operations. These components focus on intelligence gathering, capacity building, and operational coordination.

5. Regional Operations Desks: To streamline investigative efforts, Interpol operates four regional desks in Africa, Asia & the South Pacific, Europe, and the Americas. These desks are vital hubs for coordinating cybercrime research and operations within their regions.

6. Public-Private Partnership: Collaboration with private partners, including tech firms and financial organisations, is integral to Interpol's cybercrime strategy. Private partners provide valuable data and support in disrupting cybercriminal operations, bolstering Interpol's threat intelligence capabilities.

Through its collaborative approach and global network, Interpol continues to adapt to the evolving cyber threat landscape, striving to safeguard communities and uphold the rule of law in the digital age.

NCSC INTRODUCES NEW CYBER DEFENCE SERVICE AHEAD OF ELECTIONS

In a proactive move to safeguard political candidates, election officials, and other high-risk individuals from cyber threats, the UK's National Cyber Security Centre (NCSC) has launched a pioneering cyber defence service.

Here are the details of the initiative:

Personal Internet Protection Service: The newly unveiled service, announced on the second day of CYBERUK 2024, offers additional security for individual devices. It functions by alerting users about potentially malicious domains and blocking outgoing traffic to these domains, thereby fortifying users against spear-phishing, malware attacks, and other cyber threats.

Opt-In Support: Individuals at high risk of cyber targeting can opt into this service, which is part of a comprehensive cyber support package ahead of the upcoming general election. This initiative aligns with recent revelations of cyber threats by Russian Intelligence Services and China’s state-affiliated actors, highlighting the need for enhanced digital security measures.

Focus on Democracy Defenders: Acknowledging the critical role played by individuals in upholding democratic values, the NCSC underscores the importance of bolstering the defences of those targeted by cyber actors seeking to disrupt democratic processes. The service aims to safeguard candidates' and election officials' personal and official accounts, thereby minimising the risk of espionage operations.

Building on Protective DNS Service: The Personal Internet Protection service complements the existing Protective DNS service, which has been instrumental in shielding millions of public sector users from malicious domains since 2017. By expanding these protective measures to high-risk individuals, the NCSC aims to mitigate the cybersecurity risks associated with their crucial roles.

Collaborative Efforts: With the launch of this service, the NCSC and international partners from multiple countries have released new guidance to support civil society groups vulnerable to transnational repression by state-sponsored actors. This underscores the collaborative approach adopted to enhance global cybersecurity resilience, as evidenced by the recent Strategic Dialogue on the Cyber Security of Civil Society.

Urging Participation: NCSC Director Jonathon Ellison urges eligible individuals to sign up for the offered services and heed NCSC guidance to bolster their digital defences. As elections loom large on the horizon, proactive steps can now be taken to mitigate the risk of cyber threats targeting democracy defenders significantly.

As cyber threats continue to evolve, initiatives like the Personal Internet Protection service serve as critical safeguards, reinforcing the resilience of democratic institutions and individuals against malicious cyber activity.

RETHINKING THREAT DETECTION WITH AI

Traditional defence methods often prove inadequate in a dynamic digital landscape where cyber threats evolve continuously. However, Microsoft is spearheading a paradigm shift in cybersecurity through innovative AI-driven solutions.

Here's an overview of their approach:

Microsoft Security Copilot: Representing a quantum leap in AI-driven security solutions, Microsoft Security Copilot leverages generative AI to empower security professionals to detect and respond to cyber threats with unprecedented efficiency and accuracy. By harnessing vast pools of data and threat intelligence, including 78 trillion security signals processed daily by Microsoft, Copilot delivers tailored insights and streamlines response efforts.

Collaboration with Indian Government Bodies: Recognizing cybersecurity as a collaborative endeavour, Microsoft actively partners with agencies of the Government of India to enhance the nation's cyber resilience. Initiatives such as the Memorandum of Understanding with the Directorate General of Training and the ADVANTA(I)GE INDIA programme underscore Microsoft's commitment to educating and empowering cybersecurity professionals nationwide.

Distinguishing Emerging Threats: Microsoft Security Copilot revolutionises threat detection by distinguishing emerging threats from established attack patterns, thereby addressing the limitations of traditional security tools. With enhanced accuracy and speed, Copilot enables security teams to stay ahead of rapidly evolving cyber threats and streamline incident management efforts.

Continuous Validation of Device Trustworthiness: Microsoft constantly validates device trustworthiness in a dynamic environment through its Zero Trust security model. Leveraging AI technologies, Microsoft enhances real-time trust evaluations, incorporating advanced authentication methods and proactive threat protection measures.

Tailoring Cybersecurity Solutions: Microsoft collaborates closely with agencies of the Government of India to tailor cybersecurity solutions to their specific needs, leveraging AI to customise security measures for governmental entities. By integrating Security Copilot across its security suite, Microsoft streamlines operations and fosters collaboration across security and IT roles, ensuring a more secure digital environment.

Transparency and Explainability: Microsoft prioritises transparency and explainability in its AI-driven cybersecurity solutions, enabling cybersecurity professionals to comprehend the decision-making processes behind threat detection and response. By adhering to the principles of responsible AI deployment, Microsoft fosters trust and accountability in its technology offerings.

Microsoft's innovative AI-driven approach empowers Indian organisations to navigate the complex cybersecurity landscape with confidence and resilience, ensuring robust protection against evolving cyber threats.

CYBER THREATS ON THE RISE: 20% OF INDIAN USERS AFFECTED IN Q1 2024

A recent study by Kaspersky reveals that cyber threats continue to pose a significant risk to Internet users in India, with approximately 20 per cent falling victim to such attacks in the first quarter of 2024.

The study highlights the following key findings:

Prevalent Threats: Web-borne threats affected nearly 22.9 per cent of users, while 20.1 per cent were vulnerable to local threats during the same period. Browsers and social media engineering emerged as the most common web threats, with cybercriminals exploiting vulnerabilities in browsers and plugins.

Emerging Threats: The study identified the rise of file-less malware as a hazardous form of cyber threat. In these attacks, threat actors utilise legitimate tools within a system to execute cyber-attacks, bypassing the need to trick users into downloading malicious files. Social engineering techniques such as phishing, baiting, and pretexting also remained prevalent as cyberattack methods.

Magnitude of Threats: According to the Kaspersky Security Network (KSN) report, 12,454,797 Internet-borne cyber threats were blocked between January-March 2024.

Challenges for Users and Organizations: Malware remains a significant threat to users and organisations in India. Targeted malware attacks, stealth threats, and exploiting user vulnerabilities continue to pose challenges, highlighting the need for robust cybersecurity measures.

As cyber threats evolve and increase, it becomes imperative for users and organisations alike to prioritise cybersecurity and adopt proactive measures to safeguard against potential risks.

INDIAN ELECTION UNDER SIEGE: CYBER THREATS AND DATA LEAKS

Security analysts have flagged a notable surge in cyber activities targeting the Indian general election. This escalation, primarily instigated by various hacktivist factions, has led to the exposure of personally identifiable information (PII) of Indian citizens on the dark web. The election, scheduled in seven phases from April 19 to June 1, 2024, is being held for 543 seats of the Lok Sabha, with results to be announced on 4 June 2024.

Recent data from Resecurity, a cybersecurity services and solutions company based in the, indicates a significant uptick in cyber-attacks, notably since the initiation of the #OpIndia campaign last year. These attacks saw a remarkable 300 per cent spike following the #OpIsrael campaign, coinciding with heightened online protests amidst the Israel-Gaza crisis.

The growing stature of India, with its massive population exceeding 1.4 billion and a GDP of $3.41 trillion, has positioned it as a prime target for foreign threat actors and nation-state groups.

Resecurity's advisory underscores the geopolitical volatility, accentuated by conflicts in the Middle East and Eastern Europe, emphasising the imperative for secure elections to uphold global democratic stability. Their findings highlight cyberattacks on elections in over 17 countries, with India witnessing similar patterns involving data breaches, misinformation dissemination, and foreign intervention.

The security firm notified Indian authorities about the compromised voter ID cards and other sensitive data, emphasising that these breaches aim to erode trust in India’s electoral systems. The stolen data, encompassing identifying details such as AADHAAR and PAN, likely originates from compromised third-party systems utilised for know-your-customer (KYC) protocols. Cybercriminals have exploited this information to propagate narratives of vulnerability in the electoral system.

INDIA AND ESTONIA EXPLORE CYBERSECURITY COLLABORATION

Estonia, renowned as one of the world's most digitally advanced nations, seeks to forge partnerships with India in cybersecurity.

During several meetings with Indian journalist delegation in Tallinn, capital of Estonia, critical stakeholders within the Estonian Government expressed their eagerness to collaborate with India on cybersecurity initiatives.

The country faced extensive cyberattacks in 2007, notably a Distributed Denial of Service (DDoS) attack coinciding with riots following the removal of a Soviet war memorial. Since then, the country has experienced large-scale DDoS attacks, allegedly backed by Moscow, particularly after Estonia's vocal support for Ukraine following the Russian invasion.

With Estonia's rich experience in cybersecurity and India's growing digital footprint, a collaboration between the two nations holds promise in fortifying cyber defences and fostering digital resilience.

RANSOMWARE ATTACKS PERSIST IN INDIA: 64% FIRMS AFFECTED, 65% PAY RANSOM

Despite a slight decrease from the previous year, ransomware attacks continue to plague Indian organisations, with 64 per cent falling victim to such attacks, according to a report by cybersecurity solutions provider Sophos. The 'State of Ransomware in India 2024' report highlights the escalating severity of these attacks, with heightened ransom demands and recovery costs.

Derived from a survey of 5,000 IT decision-makers across 14 countries, including 500 respondents in India, the report reveals that Indian organisations are increasingly inclined to pay ransom demands (65 per cent) rather than rely on backups (52 per cent) to recover data. The average ransom demand soared to $4.8 million, with a significant portion exceeding $1 million, resulting in a median ransom payment of $2 million.

Notably, the average recovery cost for data in India amounts to $1.35 million, with 44 per cent of impacted computers encrypted and 34 per cent involving data theft alongside encryption.

Despite these challenges, 61 per cent of victims restored their data within a week, 96 per cent reported the attacks to authorities, and 70 per cent received investigation assistance.

Globally, ransomware payment trends indicate that only 24 per cent of payers remit the originally requested amount, with the average payment amounting to 94 per cent of the initial demand. Various funding sources contribute to ransom payments, with organisations covering 40 per cent and insurance providers 23 per cent.

Furthermore, the report highlights that 94 per cent of organisations affected by ransomware experienced attempts to compromise their backups, successfully infiltrating 57 per cent of the cases. Additionally, in 32 per cent of data encryption incidents, data theft occurred, amplifying attackers' leverage over victims.

In light of these findings, bolstering cybersecurity measures and enhancing resilience against ransomware attacks remain imperative for organisations in India and globally.

IFF FACILITATES INSIGHTFUL DISCUSSION ON DPDP ACT 2023 AT CIOAXIS 2024

India Future Foundation (IFF) was honoured to participate in a panel discussion at CIOAXIS's 2024 event. Led by Mr Kanishk Gaur, Founder & CEO, IFF, the debate brought together esteemed speakers Baidyanath Kumar, Chief Information Security Officer(CISO) & Data Protection Officer(DPO), JK Lakshmi Cement; Sharad Srivastava, Founder & CEO, Certus Software India; Subhash Singh Punjabi, CISO & Head Enterprise Architecture, Deepak Fertilisers and Petrochemicals Corporation; Deval M. Vishwas Pitre, Chief Information Security Officer (CISO) & Data Privacy Officer (DPO, Zensar Technologies and Arif Bhatkar, Head-IT Security, Godrej Infotech to explore the **"DPDP Act, 2023: A Dawn of A New Era For Data Protection In India."**

The panel delved into the objectives of India's new data protection legislation, comparing it to global standards such as The General Data Protection Regulation (GDPR), 2016 and discussing its profound implications for businesses, particularly regarding compliance and operational challenges.

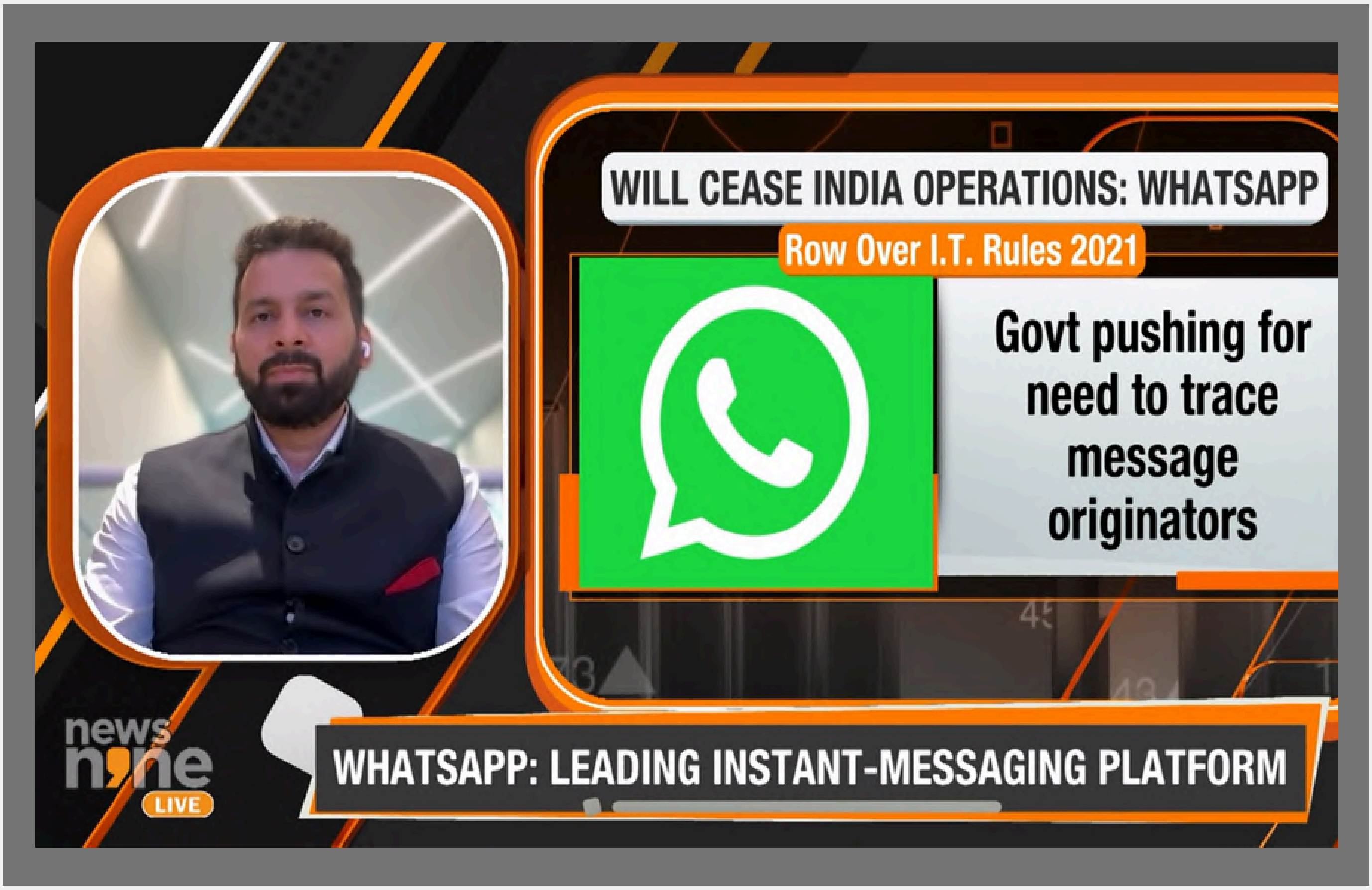
An essential aspect highlighted was the role of Data Protection Officers (DPOs), emphasising the crucial need for robust support systems within organisations to uphold the new standards effectively.

Additionally, the discussion explored data subject rights and consent practices, offering practical guidance for businesses to adapt to these changes. Complex issues like data localisation and cross-border data transfer were also addressed, providing actionable insights for organisations to navigate these regulations successfully.

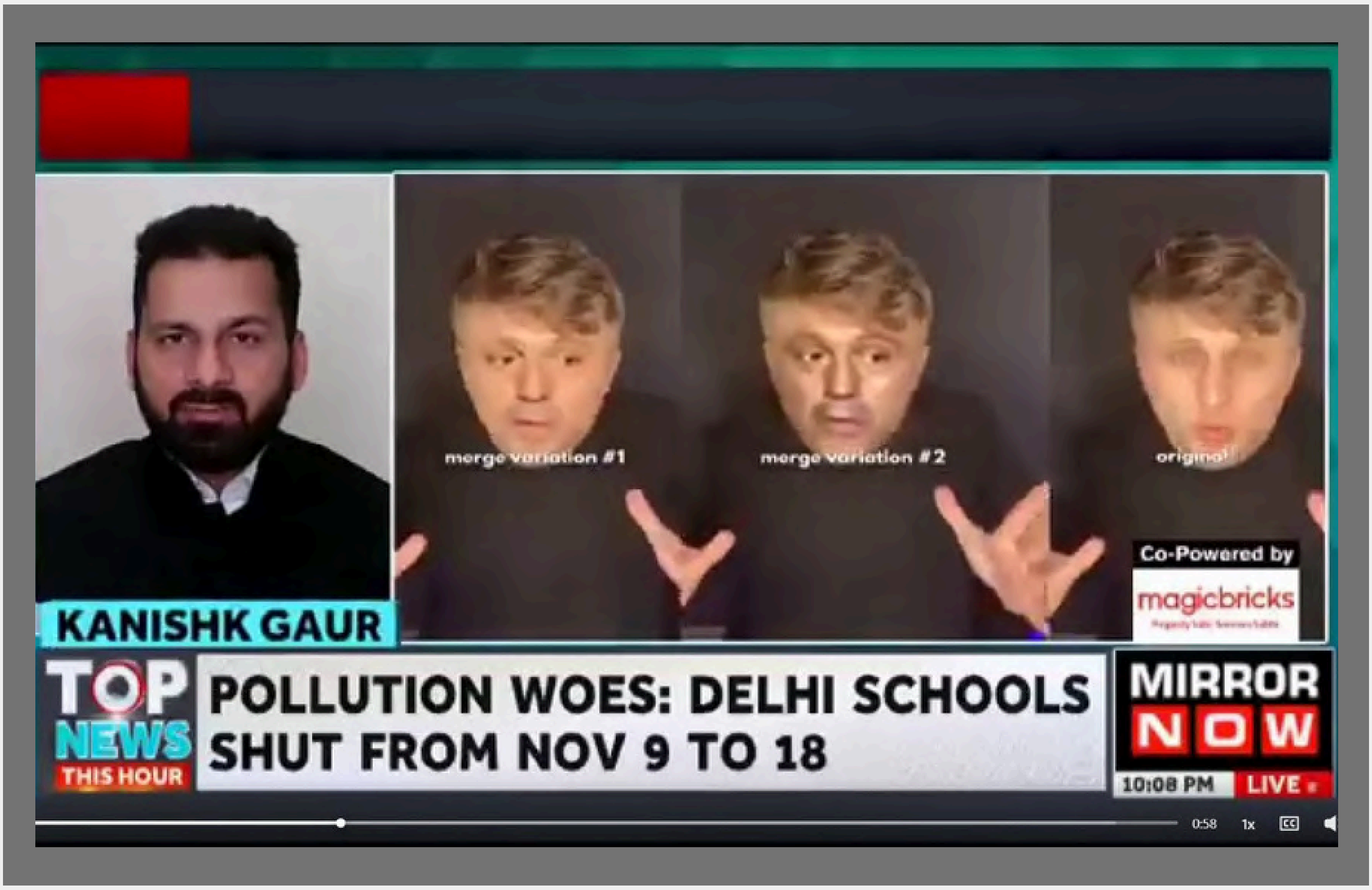
IFF is proud to have facilitated this session, which promises to shape India's data protection landscape positively.

Panel Discussion
DPDP Act 2023: A Dawn Of A New Era For Data Protection In India
MODERATOR
PANEL SPEAKERS
Kanishk Gaur
Founder & CEO, India Future Foundation
Vishwas Pitre
CISO & DPO, Zensar Technologies Ltd
Baidyanath Kumar
Global Head of Cybersecurity, TMF Groups
Arif Bhatkar
Head – IT Security, Godrej Infotech Ltd.
Subhash Singh
CISO & Head Of Enterprise Architecture, Deepak Fertilisers & Petrochemicals Corp. Ltd.
Deval Mazmudar
Cybersecurity Advisor, TJSB Bank
Sharad Srivastava
Founder & CEO, Certus Software India Pvt. Ltd
13th INFOSEC MAESTROS (CISO) AWARDS & CONFEX 2024
MAY 10, 2024 • HOTEL SAHARA STAR • MUMBAI
mazars
ManageEngine
CHECK POINT
ASSISTO AI
CERTUS ERASURE
opentext
netskope
MSP360
Hararei
Data Resolve
4T
Neo
NEXTNINJA
CIOAXIS
CIOAXIS
CIOAXIS
CIOAXIS
CIOAXIS

IFF IN THE MEDIA


WILL CEASE INDIA OPERATIONS: WHATSAPP
Row Over I.T. Rules 2021
Govt pushing for need to trace message originators
news nine LIVE
WHATSAPP: LEADING INSTANT-MESSAGING PLATFORM

Kanishk Gaur, Founder & CEO, IFF, shared his insights on National Security vs. Personal Privacy on News9 Plus.



Kanishk Gaur, Founder & CEO, IFF, discussed Deepfake Technology 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