INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on the Internet

NEWS FROM AROUND THE WORLD

2023: A YEAR OF CYBERSECURITY TRIUMPHS AND TRIBULATIONS

2023 was a year when the digital world saw the best and worst of cybersecurity. From groundbreaking initiatives to alarming trends, let's delve deeper into six stories that shaped the online security landscape:

1. US National Cybersecurity Strategy: Building a Fortified Cyberspace

President Biden unveiled a comprehensive National Cybersecurity Strategy in March 2023, recognizing the escalating cyber threats. This ambitious plan aims to:

Bolster defences: Strengthen critical infrastructure like power grids and financial systems against cyberattacks.

Enhance government protection: Improve cyber defences across federal agencies and share intel with private companies.

IN THIS NEWSLETTER

Foster global collaboration: Work with international partners to combat cybercrime and develop norms for responsible behaviour in cyberspace.

This strategy represents a significant step towards making cyberspace more secure and resilient. It's a welcome shift towards a proactive approach, recognizing that cyber threats are a national security imperative.

2. Operation Cookie Monster Crumbles Dark Web Empire

In June 2023, a global law enforcement operation codenamed "Operation Cookie Monster" dealt a significant blow to cybercrime. The target? Genesis Market is a notorious online marketplace for stolen credentials and illegal goods.

Over a dozen international agencies collaborated to shut down the platform, seizing:

- millions of stolen logins and financial records
- countless illegal items for sale, including drugs and malware
- servers and infrastructure powering the marketplace

This takedown represents a significant victory against cybercrime. It demonstrates the power of international cooperation and sends a message to online criminals that no dark web market is genuinely beyond reach.

3. The "Right to be Forgotten" Gains Momentum

The question of controlling one's digital footprint intensified in 2023. A Canadian court ruling recognized the "right to be forgotten," allowing individuals to request the removal of personal information from search results.

This ruling sparked both cheers and concerns. Proponents: Celebrate increased privacy and control over online reputations. **Opponents:** Worry about censorship and suppression of information, particularly regarding historical records or public figures.

The "right to be forgotten" debate is far from over. It raises crucial questions about balancing privacy rights with freedom of information and accountability in the digital age.

4. The Biggest DDoS Storm Ever Hits the Web, Exposing Vulnerabilities

October 2023 saw a record-breaking distributed denial-of-service (DDoS) attack targeting internet giants like Google and Amazon. Hackers flooded these platforms with bogus traffic, aiming to overwhelm their servers and make them inaccessible to legitimate users.

This unprecedented attack highlights several vital concerns. Some of them are mentioned below.

Escalating sophistication: Cybercriminals are developing increasingly powerful tools to disrupt online services.

Critical infrastructure vulnerability: The attack targeted significant Internet providers, potentially impacting millions of users and businesses.

Better preparedness: Companies and governments must invest in more robust defences and contingency plans to withstand future attacks.

The "DDoS storm" is a wake-up call for the entire digital ecosystem. It underscores the need for proactive security measures and global collaboration to protect critical infrastructure and ensure online stability.

5. Gathering Cyber Storm Warns of Looming Threats Urging Proactive Measures

Experts at the World Economic Forum's Annual Meeting in Davos 2023 sounded the alarm about a "gathering cyber storm." This storm, they warned, is fuelled by the following:

Geopolitical tensions: Increased cyberattacks between nations and state-sponsored hacking groups.

Advanced AI tools: Hackers harness the power of artificial intelligence to automate attacks and develop more sophisticated malware.

Cybersecurity skills gap: A shortage of skilled professionals to defend against increasingly complex threats.

This bleak picture emphasizes the need for immediate action, which includes the following:

Global cooperation: International collaboration is crucial to counter cybercrime and develop collective defence strategies.

Investment in AI security: Research and development are needed to protect against AI-powered attacks.

Bridging the cybersecurity skills gap: Governments and businesses must invest in training programmes and workforce development initiatives.

Ignoring the "gathering cyber storm" is not an option. Proactive measures and a united front are essential to weather the coming challenges and ensure a secure future for the digital world.

6. The Cybersecurity Skills Gap Widens, Threatening Global Security

The demand for cybersecurity professionals continues to outpace supply, creating a critical skills gap that jeopardizes national security and economic stability. According to the World Economic Forum, the global workforce needs an estimated 3.4 million additional cybersecurity experts to protect today's digital infrastructure.

This shortage is particularly acute in critical sectors like energy utilities, healthcare and financial services, where cyberattacks can have devastating consequences. Several factors contribute to the skills gap, which are mentioned below:

Rapid technological advancements: Cyber threats evolve quickly, requiring constant skill updates.

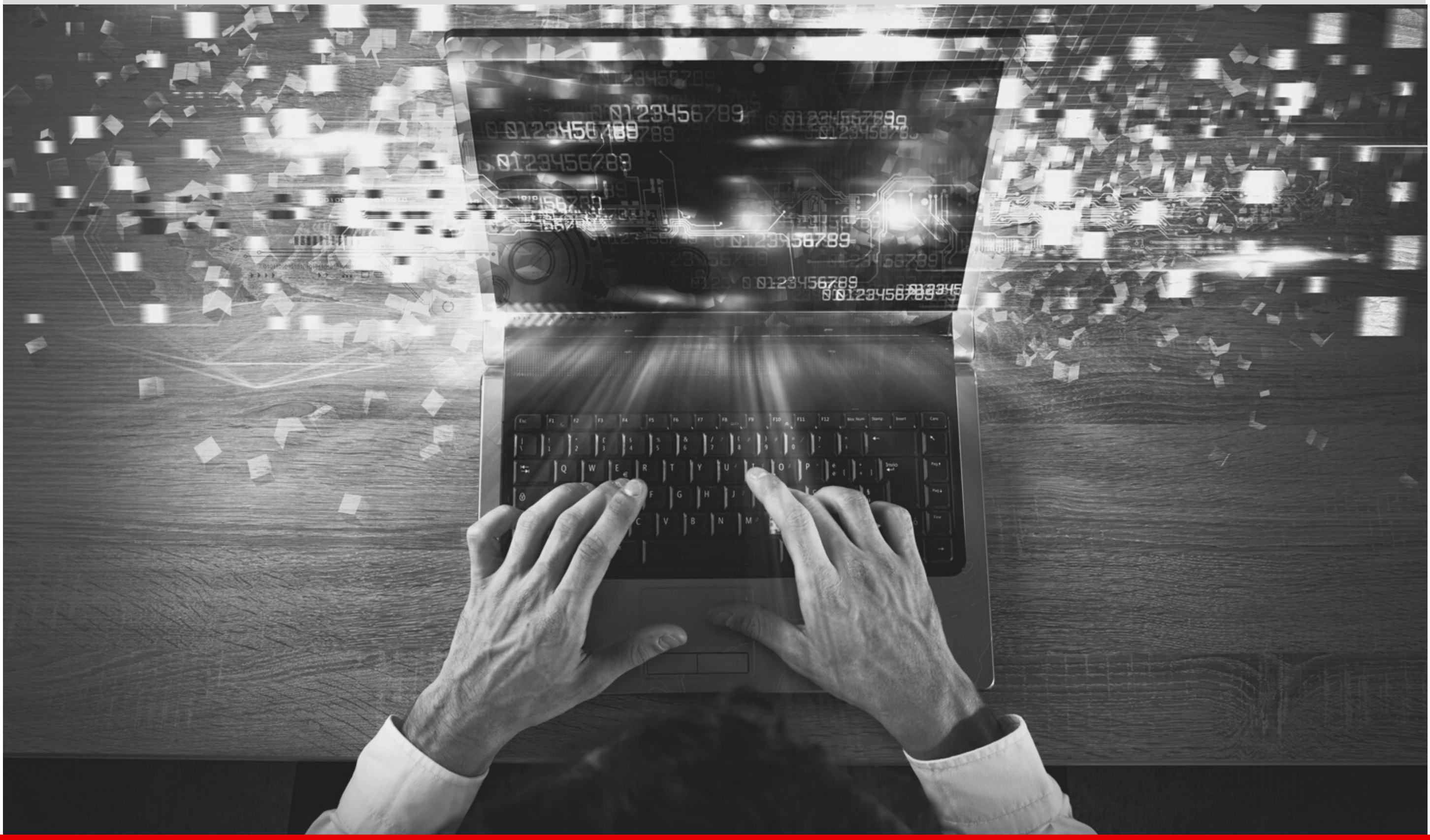
Lack of awareness and education: Many people lack cybersecurity career paths or the necessary training.

Competition from other industries: Tech companies often attract talent with higher salaries and benefits.

To bridge this gap, concerted efforts are needed, which are mentioned below:

- **Education and training:** Increasing cybersecurity courses in schools and universities, offering professional development programmes for existing IT professionals, and providing hands-on training opportunities through internships and apprenticeships.
- **Industry-academia partnerships:** Fostering collaboration between businesses and educational institutions to align curricula with industry needs and provide students with real-world experience.
- **Diversity and inclusion initiatives:** Broadening the talent pool by attracting women and underrepresented groups to cybersecurity careers.
- **Government support:** Offering cybersecurity education and training incentives, funding research and development in cybersecurity technologies, and establishing clear career pathways.

Addressing the cybersecurity skills gap is not a one-time fix; it requires sustained commitment from governments, businesses, and educational institutions. By investing in developing a skilled cybersecurity workforce, we can better protect our digital infrastructure and create a safer, more resilient online world.



TOP DATA BREACHES OF 2023: A GLOBAL PERSPECTIVE

2023 saw a series of significant data breaches, highlighting the critical need for robust cybersecurity measures across industries and nations. Here's a glimpse into some of the most significant incidents:

Global

MOVEit Cyberattack: Over 2,000 organizations worldwide, including government agencies and major companies, were compromised by a ransomware attack exploiting a vulnerability in Progress Software's file transfer protocol. The attack sparked concerns about supply chain security and prompted the U.S. SEC to tighten disclosure requirements for cyber incidents.

Aadhaar Data Breach (India): Up to 815 million Indian citizens' personally identifiable information, including their Aadhaar numbers and passport details, were reportedly sold on the dark web, raising concerns about the security of India's national identity system.

United States of America

Boeing Data Leak: A cybercrime gang published internal data, online, from Boeing, a leading aerospace giant, after a ransomware attack. While Boeing assured us there was no threat to flight safety, the incident raised concerns about data protection in critical infrastructure sectors.
23andMe Genetics Breach: Hackers compromised the "DNA Relatives" feature of the famous genetic testing company, potentially exposing the genetic data of millions of users. This highlighted the vulnerability of personal health information in the digital age.

Others

17,000 WordPress Sites Hacked: A series of cyberattacks targeted WordPress websites, exploiting vulnerabilities in popular themes like Newspaper and Newsmag. This highlighted the importance of updating software and plugins to prevent such exploits.

Impact and Lessons Learned

These incidents underscore the evolving landscape of cyber threats and the need for proactive security measures. Organizations and governments must do the following:

Impact and Lessons Learned

These incidents underscore the evolving landscape of cyber threats and the need for proactive security measures. Organizations and governments must do the following:

The year 2023 is a stark reminder that data security is an ongoing challenge. We can strive towards a more secure digital future by adopting robust measures and fostering international collaboration.

The year 2023 is a stark reminder that data security is an ongoing challenge. We can strive towards a more secure digital future by adopting robust measures and fostering international collaboration.

CHINA STRENGTHENS DATA SECURITY

China has taken a crucial step towards bolstering data security within its borders by proposing a comprehensive four-tier contingency plan. This move comes in light of increasing concerns about large-scale data leaks and cyberattacks, including the high-profile incident last year, in July 2022, involving the alleged theft of personal information from the Shanghai police.

The draft plan, outlined by the Ministry of Industry and Information Technology (MIIT) on 15 December 2023, establishes a color-coded system to categorize data security incidents based on their severity. The tiers range from "green" for minor incidents to "red" for the most critical situations, which involve significant financial losses exceeding 1 billion yuan (approximately $141 million) and potential compromise of sensitive data affecting millions of individuals.

The new system has implemented a hierarchical categorization for data security incidents based on their scope and severity. The four levels, as per the new plan, are as follows:

Red (Level I - Especially Significant): This level applies to events resulting in widespread shutdowns, major economic losses (amounting to over 1 billion yuan), or compromising personal information of over 100 million individuals. It is activated when there are serious anomalies lasting more than 24 hours.

Orange (Level II - Significant): This level is activated for situations such as shutdowns and operational interruptions that exceed 12 hours but less than 24 hours. This grade of severity applies to economic losses between 100 million and 1 billion yuan, or when personal information of over 10 million individuals, but less than 100 million individuals, is compromised.

Yellow (Level III - Large): This severity level is applicable when events that cause operational interruptions lasting over eight hours (but less than 10 hours) and results in economic losses ranging from 50 million to 100 million yuan. This grade of severity is applicable when personal data of more than 1 million individuals (but less than 10 million) is impacted.

Blue (Level IV - General): This level pf severity is for minor events that cause less significant operational interruptions and economic losses, in this level of severity, is under 50 million yuan. It applies to incidents that affect the personal data of less than 1 million individuals.

For incidents that fall in the severity of red and orange, the plan mandates stringent measures, that include the following:

- 24/7 response teams: Companies and local regulators must establish dedicated teams to address the incident round the clock.
- Immediate notification: Data breaches must be reported to MIIT within ten minutes of their occurrence.
- Strict reporting requirements: Any delay, falsification, or concealment of reporting is strictly prohibited and could face consequences.

This emphasis on prompt and transparent communication highlights China's commitment to rapid response and effectively containing data security threats. The plan also outlines responsibilities for various stakeholders, including government agencies, companies and individuals, ensuring a co-ordinated and comprehensive approach to data protection.

While the draft plan seeks public feedback, its implementation is expected to enhance China's data security posture significantly. This strengthens national security and individual privacy and fosters trust in the digital economy. The plan's emphasis on timely reporting and accountability aligns with international best practices and sets a positive precedent for data governance in the global landscape.

UKRAINE'S BIGGEST MOBILE NETWORK BACK ONLINE

After a significant cyberattack disrupted services for millions of Ukrainians on 12 December 2023, Kyivstar, the country's largest mobile operator, has successfully restored all communication channels. The attack, which is believed to be linked to the Russian military intelligence, targeted the company's IT infrastructure and even impacted air raid alert systems in some areas.

Undeterred, Kyivstar engineers worked around the clock to bring the network back online. Within a week, they fully restored mobile Internet, voice and SMS services, operating at 100% capacity in Ukraine and abroad. This swift response is a testament to the company's dedication and the resilience of the Ukrainian people.

Kyivstar CEO Oleksandr Komarov hinted that there were major learnings from the incident, which suggest that the company would take steps to bolster its cybersecurity measures, using the experience gained from this experience and could potentially extend insights to other organizations. The attack reportedly exploited a compromised employee account, although the details remain undisclosed. Kyivstar assured its customers that no personal data was compromised during the incident.

While the attack served as a stark reminder of the vulnerabilities present in today's digital world, Kyivstar's swift and successful restoration of services highlights the importance of robust cybersecurity measures. This incident also showcased the unwavering determination of the Ukrainian people in the face of adversity.

AUSTRALIAN COURT PROCEEDINGS RECORDING DATABASE BREACHED

A significant cyberattack rocked Victoria, Australia, compromising the state's court recording database and potentially exposing sensitive information from countless legal proceedings. This incident raises serious concerns about data security, privacy and the justice system's integrity.

Details of the Breach.

Hackers gained unauthorized access to the database, potentially stealing recordings of court hearings between 1 November 2023 and 21 December 2023. The full extent of the data that was stolen and the identities of the perpetrators remain unknown, and there is a possibility that court proceedings prior to November 1 may have also been compromised.

The breach was confirmed on 2 January 2024, by Louise Anderson, CEO, Court Services Victoria, who assured that no other court systems or records, including employee or financial data, were accessed by the perpetrators. Court Services Victoria collaborates with government cybersecurity experts to investigate the attack, assess the damage, and mitigate potential consequences.
The possibility of ransom demands by the hackers has not been publicly disclosed.

Potential Impact.

The stolen recordings could contain a wealth of sensitive information, including personal details of individuals involved in legal cases, such as victims, witnesses and defendants. The leaked data could compromise ongoing investigations and witness protection efforts.
This breach can erode public trust in the justice system and its ability to ensure fair and secure legal proceedings.

Wider Concerns.

The attack echoes recent cyberattacks targeting critical Australian infrastructure, highlighting the nation's increasing vulnerability to malicious actors. In late 2023, a cyberattack crippled operations at DP World Australia, one of the country's largest seaports and car dealership group Eagers Automotive also became victim of a cyber incident.

A government report from November 2023 revealed the alarming frequency of cyberattacks in Australia, with an average attack occurring every six minutes.

Going Forward.

Court Services Victoria is immediately restoring affected systems, enhancing security measures and preventing future intrusions.

The Government of Australia is expected to intensify efforts to bolster cybersecurity defences and protect critical infrastructure from cyber threats. This incident underscores the urgent need for robust data security protocols, increased vigilance against cyberattacks and international cooperation to combat cybercrime.

QR CODE PHISHING ON THE RISE

QR codes, once seen as a quick and convenient way to access information, are increasingly being weaponized by cybercriminals for phishing attacks. This trend, known as "quishing," raises serious concerns about data security and online safety.

QR codes, are the scannable squares promising instant access to websites, menus, or coupons, that have become ubiquitous these days. Their user-friendly nature and adaptability have positioned them as a beloved choice among marketers and consumers. However, this very popularity has attracted the attention of malicious actors who have weaponized these seemingly innocuous squares.

Cybercriminals increasingly embed malicious links within QR codes, leading unsuspecting users to fake websites that steal login credentials and financial information or even infect devices with malware. These attacks, cleverly dubbed "quishing," bypass traditional email security checks, making them difficult to detect and particularly effective against mobile devices.

Scope of Threat.

- Exponential growth: Reports indicate a significant rise in quishing attacks, with some estimates suggesting a 50% increase in September 2023, over the cumulative figure of the previous eight months.
- Varied targets: From individual consumers to corporate employees, quishing attacks can target anyone with a smartphone who has a penchant for scanning.
- Multifaceted threat: Credential phishing, invoice scams and even ransomware distribution are some ways in which quishing can wreak havoc.

Staying Safe in a World of QR Codes.

Amidst the rising threat, vigilance and awareness are the key. Here are some tips to navigate the QR code landscape safely:

- Think before you scan: Don't mindlessly scan QR codes, especially those encountered in unsolicited emails or public places.
- Verify the destination: Hover your camera over the code (if possible) to see a preview of the URL it leads to. Look for suspicious domain names or mismatched website titles.
- Use trusted applications: Consider using QR scanning applications with built-in security features that can detect malicious links.
- Context matters: If a QR code appears out of place, it's best to avoid it altogether.
- Trust your instincts: If something feels off, it probably is. Don't hesitate to err on the side of caution and walk away.

QR codes, while providing convenience, are not without risks. By understanding the threat of quishing and adopting a cautious approach, we can ensure that these squares remain a convenient tool, not a gateway to cybercrime.

THE OKTA BREACH

Okta, a leading identity and access management platform, recently revealed a massive breach affecting 18,400 customers.

Here are the key takeaways for CISOs.

- **Scope:** The breach impacted all 18,400 Okta customers, not just the 1% initially reported. This includes high-profile names like FedEx, Zoom and HPE.
- **Exposure:** Hackers gained access to the names and email addresses of all Okta customer support system users, increasing the risk of phishing and social engineering attacks.
- **Recommendations:** Okta advises implementing multi-factor authentication for admins, enforcing session timeouts and binding and conducting phishing awareness training.
- **Lessons Learned:** The breach highlights the need for stricter security practices, including:
  - BYOD policy review: Consider the risks associated with personal accounts on business devices.
  - Employee training: Train employees on best practices to identify and mitigate cyber threats.
  - Enterprise browsers: Explore secure, enterprise-grade browsers that offer greater control over user activity.
- Rebuilding Trust: Okta faces a long road to regain trust after this incident. Transparency and timely updates are crucial to rebuilding customer confidence.
- Alternative Solutions: Some Okta customers may consider switching to competitor identity management providers.

This breach is a stark reminder of the ever-evolving threat landscape and the importance of robust security measures. CISOs should take this opportunity to reassess their security posture and implement necessary safeguards to protect their organizations from similar attacks.

The breach originated from an Okta employee using a personal Google account on a company laptop, highlighting the dangers of co-mingling personal and professional activities.

Forrester analyst Merritt Maxim suggests that companies should put pressure on the vendors to disclose breaches promptly and provide information on available patches and fixes.

Okta is facing a tough year with two major breaches in recent months, raising concerns about its security practices.

Cybercriminals are capitalizing on the excitement surrounding Black Friday and Cyber Monday (Black Friday is the day after Thanksgiving and is widely considered the beginning of the holiday shopping season), unleashing a surge of phishing emails designed to lure unsuspecting shoppers into revealing their personal information. These emails often mimic the look and feel of legitimate messages from well-known brands, making them difficult to distinguish from the real deals.

Security experts have observed a staggering 237% increase in these phishing attempts in the weeks leading up to the significant shopping events. Attackers craft genuine looking emails incorporating official logos, footers and even some legitimate links to the brand's website. However, in doing so, they skillfully embed at least one malicious link, often disguised as a tempting call to action button offering a discount or exclusive offer. Clicking this link can lead to a fraudulent website that captures sensitive data, of unsuspecting consumers.

To protect yourself from these scams, exercise caution and vigilance when opening emails and clicking links, especially during this peak shopping season. Here are some essential safeguards to keep in mind:

- Scrutinize links: Before clicking any link, hover your mouse over it to reveal the destination URL. Pay close attention to any discrepancies in the domain name or website title.
- Verify the sender's authenticity: Don't trust an email simply because it appears to originate from a familiar brand. Examine the sender's email address meticulously, looking for any typos or inconsistencies that could indicate a fake.
- Be wary of urgent language: Scammers often employ tactics to create a sense of urgency, such as highlighting limited-time offers or expiring deals. This sense of pressure can cloud judgment, so proceed with caution when encountering such language.
- Never enter personal information in emails: Legitimate businesses will not request sensitive data like login credentials or financial details directly through email. If asked to provide such information, it strongly indicates of a scam.
- Prioritize trusted shopping platforms: To minimize risks, stick to reputable retailers and marketplaces with a proven security and trustworthiness track record.
- Report suspicious emails: If you encounter an email that raises red flags, take action by forwarding it to the brand it impersonates or reporting it to your email provider. This proactive step helps combat the spread of these scams.

FINANCE MINISTER CALLS FOR CYBER SHIELD

On 31 December 2023, Ms Nirmala Sitharaman, Union Finance Minister, delivered a clarion call for proactive cybersecurity measures and stringent security protocols to safeguard the integrity of India's domestic financial systems. The Minister chaired a crucial review meeting with Public Sector Banks (PSBs) where she outlined a multi-pronged approach to fortify the financial ecosystem against evolving cyber threats.

Key takeaways from the call are as follows:

- Cybersecurity at the Forefront: Recognizing the growing sophistication of cyber threats targeting financial institutions, Ms Sitharaman emphasized the need for proactive and robust cybersecurity measures. This includes implementing stringent security protocols, investing in advanced tools and technologies and fostering a culture of cyber awareness within the banking sector.
- Collaboration is the Key: The Union Finance Minister stressed on the importance of collaboration between various stakeholders. She urged PSBs to coordinate closely with the National Asset Reconstruction Company (NARCL) to expedite the onboarding of stressed accounts, reducing vulnerabilities within the financial system. Additionally, she encouraged active collaboration between banks, security agencies, regulatory bodies and technology experts to create a comprehensive defence against cyberattacks.
- Combating Fraud and Promoting Responsible Lending: Ms Sitharaman commended the improved performance of PSBs but called for sustained focus on fraud prevention activities. She directed PSBs to undertake consumer education initiatives and implement stricter due diligence processes before disbursing loans. This two-pronged approach protects financial institutions and borrowers from fraudulent activities and promotes responsible lending practices.
- Building a Resilient Future: The Finance Minister's vision extends beyond immediate measures. She envisions a resilient financial ecosystem that is equipped to withstand future cyber threats. This requires continuous investment in research and development, upskilling the workforce in cybersecurity best practices and fostering a collaborative environment where information sharing and threat intelligence are seamlessly integrated.

Ms Sitharaman's emphasis on cybersecurity marks a significant step towards securing India's financial future. By proactively addressing cyber vulnerabilities and strengthening collaboration, the government aims to create a robust and resilient financial ecosystem that benefits all stakeholders.

DECIPHERING THE TAJ HOTELS BREACH

In 2023, India made rapid strides in the realm of technology, but an alarming surge in data breaches, including that of the high-profile case of Taj Hotels besmirched this progress. Owned by the Tata Group, the luxury chain fell victim to a cyberattack on 23 November 2023, compromising personal information of over 1.5 million customers.

The data that was exposed , in the breach, contained personal information of 1.5 million customers. It is possible that considering the high profile customers that the luxury chain caters to, breach of such huge amount of data, could put at risk, many high profile companies.

Using the alias "Dnacookies", the hacker demanded $5,000 for the stolen data on a dark web marketplace called Breachforums. Though hotel authorities maintained that the leaked information was non-sensitive, the lack of transparency raised concerns about the extent of damage and the potential misuse of this data.

This year, breaches have occurred across sectors, from startups to government databases. Contributing factors include third-party reliance, internal inconsistency in security practices, personal data access, and interconnected systems within large corporations.
India must adopt proactive strategies to fortify its cybersecurity defences, including comprehensive cybersecurity strategies, transparency and trust, cybersecurity investments and collaboration and knowledge sharing.

US, INDIA AND TAIWAN COLLABORATE TO BOLSTER CYBERSECURITY

American, Indian and Taiwanese cybersecurity officials joined forces to combat escalating cyber threats from China. The People's Liberation Army (PLA) intensified the development and training of various agencies for potential cyberattacks.

In a workshop hosted under the Global Cooperation and Training Framework (GCTF), representatives from the three nations, mentioned above, convened for the first-ever in-person programme held, in India. The event was co-hosted by US Ambassador Eric Garcetti, Taiwan's Representative Baushuan Ger, Lt Gen. (Retd) Dr Rajesh Pant (former National Cyber Security Coordinator of India) and the National Security and Defence Services think tank, United Service Institution of India (USI).

Highlighting the shared concern over cyber threats originating from China, Ambassador Garcetti emphasised on the commitment of the United States of America to collaborate closely with partners like India and Taiwan. Lt Gen. (Retd) Dr Pant underscored India's recognition of cybersecurity as a pivotal aspect of national security, particularly with over 800 million Internet users and 1.2 billion smartphones.

The Global Counterterrorism Forum (GCTF), initiated in 2015, has conducted numerous international workshops to enhance collaboration among experts in various fields, including cybersecurity. Taiwan's expertise, despite global recognition, faces limitations due to pressure from Beijing on international institutions, hindering its active participation. The platform, however, allows practitioners worldwide to tap into Taiwan's knowledge pool and foster cross-border connections to address contemporary challenges.

Despite political hurdles, the collaboration between the USA, India and Taiwan signifies a collective effort to fortify cybersecurity measures in an increasingly interconnected digital landscape.

AI - HORIZONS: HARNESSING AI TO COUNTER CYBER THREATS

IFF in association with Microsoft organised a seminar— AI Horizons – Harnessing the Power of AI to Counter Cyber Threats—on 11 December 2023 at Regal, The LaLiT, from 11 AM to 2 PM.

The event explored the potential of AI to infer, recognise patterns and take proactive measures to make the Internet a safer place for all, from cyberattacks, especially by harnessing the potential of artificial intelligence (AI).

This included enhancing incident response time, refining threat detection mechanisms, analysing extensive data sets, and more.

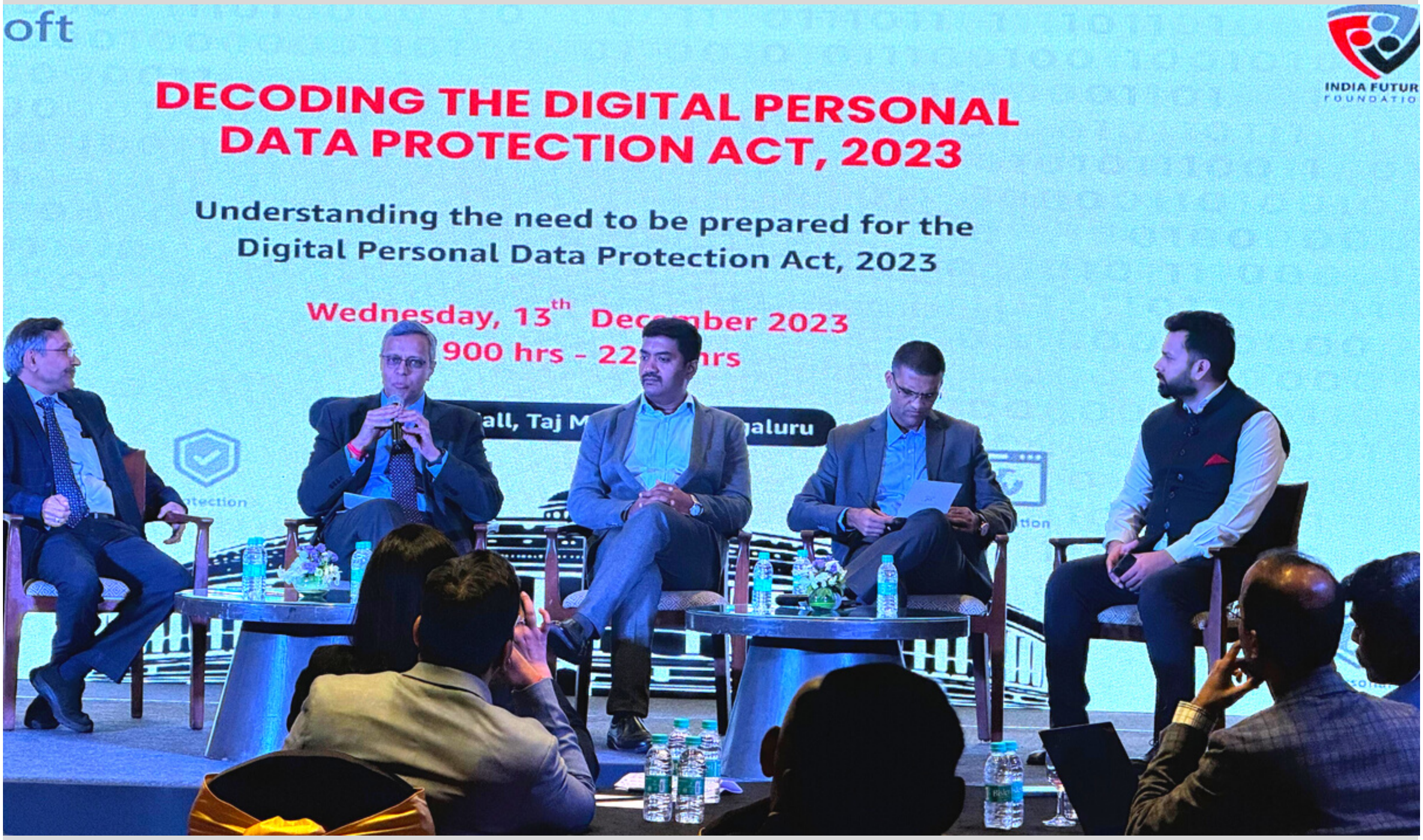
The discussions at the event encapsulated the following pivotal areas:

- **Proactive Measures:** Emphasize AI's role in real-time threat detection and automated incident response as a critical deterrent against cyber threats.
- **Ethical Deployment:** The focus was on ensuring AI's ethical use, transparency, and upholding stringent data privacy standards within organisational frameworks.
- **Skillset Development:** Recognize the necessity for a robust cybersecurity skillset among professionals to use AI-driven tools effectively.
- **Business Strategies:** Underline the significance of AI-powered cybersecurity strategies in fostering transparency, accountability and confidence among businesses and stakeholders.
- **Big Tech's Contribution:** Acknowledge the pivotal role of major tech companies in propelling innovation in AI and establishing standardised ethical frameworks for robust cybersecurity measures.

IFF expressed gratitude to the panellists, Gen. (Retd) (Dr) Manoj Mukund Naravne, Former Chief of Army Staff, Indian Army; Lt Gen. (Retd) Vinod G. Khandare, Principal Advisor, Ministry of Defence, Government of India; Mr Jayant Misra, Consultant, United Nations Office on Drugs and Crime, Regional Office South Asia; Dr BULUSU Krishna Murthy, Former Senior Director (Scientist G) & Group Coordinator (R&D in IT), Ministry of Electronics and Information Technology (MeitY), Government of India; Col (Retd) Sanjeev Relia, Chief Strategy Officer, ThinkCyber India; Col (Retd) Suhail Zaidi, Director General, MAIT (apex body representing India's electronics & ICT hardware sector); Mr Binu George, Head-Government Affairs-India, Fortinet; Prof. Anjali Kaushik, Former Dean, and Chair, CoE on Digital Economy and Cyber Security (DECCS), Management Development Institute, Gurgaon; Mr Alok B. Lall, National Security Officer – India & South Asia, Microsoft; Mr Salil Mittal, Lead Cyber Security, Jio; Mr Michael Calegari, Special Agent, Drug Enforcement Administration, American Embassy; Ms Lana M. Worobec, Supervisory Investigator (Chemicals/Pharmaceuticals), Drug Enforcement Administration, American Embassy and Mr Sambhav Dang, Narcotics Investigator – India, Bangladesh, Bhutan, Maldives, Nepal, Sri Lanka, United States Embassy; Commander (Retd) Sandeep Padam, Cyber Security Expert; Dr Shruti Mantri, Associate Director, Indian School of Business, Hyderabad; Dr Abhinav Dhall, Head of Data Science, IIT Ropar and Mr Devesh Verma, VP & Deputy Head of Cyber COE, for sharing their views on the integration of Artificial Intelligence with Cybersecurity, thereby making complex concepts easy to understand.

IFF also expressed profound gratitude to those behind the scenes who worked tirelessly to make the event successful. Kanishk Gaur, CEO, IFF; Pankaj Anup Toppo, Head-Policy Programmes & Research, IFF; Rakesh Maheshwari, Former Senior Director and General Counsel of Cyber Law at the Ministry of Electronics and Information Technology (MeitY) and presently, Member Advisory Board, IFF; Manmeet Randhawa, Head-Corporate Communication & Strategic Alliances, IFF; Sanjeev Relia, Chief Strategy Officer, ThinkCyber India, and Nikhil Bansal, Deputy Manager, IFF, provided invaluable support and guidance, ensuring everything ran smoothly.

DECODING THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 RIZONS: HARNESSING AI TO COUNTER CYBER THREATS (BENGALURU CHAPTER)


oft
DECODING THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023
Understanding the need to be prepared for the Digital Personal Data Protection Act, 2023
Wednesday, 13th December 2023
900 hrs - 22 hrs
all, Taj M aluru
INDIA FUTURE FOUNDATION

India Future Foundation (IFF) and Microsoft hosted an enlightening panel discussion on the implications of the Digital Personal Data Protection Act, 2023, on 13 December at the Taj MG Road, Bengaluru.

The session featured luminaries from the tech and legal sectors, who provided invaluable insights that helped navigate the complexities surrounding this landmark legislation.

Mr Rakesh Maheshwari, Former Senior Director and General Counsel of Cyber Law at the Ministry of Electronics and Information Technology (MeitY), Government of India and presently, Member Advisory Board, IFF, led the discussions, articulating essential steps for companies to embark on their compliance journey with the DPDP Act, 2023. His expertise, in the said field, delved into the intricacies of the Act, highlighting the legislation's role in safeguarding digital personal data and nurturing the digital ecosystem.

Ms Vasantha Lakshmi, Technology Specialist – Security and Compliance, Microsoft, elucidated technical solutions to assist Indian businesses in aligning with the DPDP Act, showcasing Microsoft's commitment towards data protection.

The dialogue witnessed an enlightening discussion among industry leaders, including Mr Alok B. Lall, National Security Officer – India & South Asia, Microsoft; Mr Lahar Appaiah, Legal Counsel, IBM India and South Asia and Mr Malligarjunan Easwaran, Sr Cybersecurity Architect – WW Cybersecurity Practice, Hewlett Packard Enterprise. Insights provided by them, on the matter, provided a comprehensive understanding of the Act and how this Act offers strategic guidance for businesses. The panel addressed implementation mechanisms, debating their efficacy in ensuring compliance and providing a holistic view of the DPDP Act's implementation.

IFF expressed gratitude for the active participation of Mr Kapil Mehrotra, the then Group CTO & CISO, Dhanuka Agritech Ltd; Mr Kanishk Gaur, Founder, IFF; Ms Manmeet Randhawa, Head- Corporate Communications & Strategic Alliances, IFF and Mr Nikhil Bansal, Deputy Manager, IFF. Their contributions played a crucial role in the event's success.

DECODING THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (DELHI CHAPTER)

Microsoft
DECODING THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023
Understanding the need to be prepared for the Digital Personal Data Protection Act, 2023
INDIA FUTURE FOUNDATION
THE LaLiT

IFF and Microsoft organised an awareness seminar on decoding the Digital Personal Data Protection Act 2023 on 22 December 2023 at Regal, The LaLiT, from 06:30 PM to 9 PM.

The seminar was more than just a knowledge-sharing platform; it catalysed change. The seminar empowered individuals and organisations to navigate the DPDP Act, 2023, confidently by fostering open dialogue, sharing best practices and providing actionable insights. It was a launch pad for building a future where responsible data governance paves the way for innovation, trust and individual empowerment in this digital age. The event provided valuable insights into the Act's implications for various stakeholders.

The event touched upon various facets, which included the following:

Clarity on core principles: The event offered clear explanations of the core principles of the DPDP Act, 2023, such as consent mechanisms, data minimisation and accountability, dispelling confusion, and providing organisations with a roadmap for compliance.

Understanding sectoral impact: Different industries face unique challenges under the DPDP Act, 2023. The event explored how the Act affects sectors like healthcare, finance and technology, enabling participants to identify and address their specific data governance hurdles.

Building a roadmap for compliance: The event provided practical guidance on developing effective compliance strategies, designing robust data governance models, implementing technical safeguards, and building a data protection culture within organisations.

Leveraging Microsoft's expertise: Microsoft, a global leader in technology and data security, offers tools and products to support organisations in their compliance journey with the DPDP Act, 2023. The event showcased how Microsoft can be a valuable partner in this endeavour.

IFF highly acknowledges the contribution of the speakers, Lt Gen. (Retd) Vinod G. Khandare, Principal Advisor, Ministry of Defence, Government of India; Dr Yusuf Hashmi, Group Chief Information Security Officer (CISO), Jubilant Bhartia Group; Dr Yask Sharma, Chief Information Security Officer (CISO), Indian Oil Corporation Limited (IOCL); Mr Amit Dhingra, Senior Vice President-Risk & Compliance, HCL Tech; Mr Nagender Singh, Joint Director (IS-NDR), Hindustan Petroleum Corporation Ltd. (HPCL); Mr Kinshuk De, Senior Consultant, Tata Consultancy Services (TCS) and Mr Alok B. Lall, National Security Officer – India & South Asia, Microsoft for sharing their views on the matter at the consultation.

IFF also acknowledges the participation of Mr Kanishk Gaur, Founder, IFF; Mr Rakesh Maheshwari, Former Senior Director and Group Co-ordinator, Cyber Laws and Data Governance, Ministry of Electronics and Information Technology (MeitY), Government of India and presently Member, Advisory Board, IFF; Mr Pankaj Anup Toppo, Head – Policy Programmes & Research, IFF; Ms Manmeet Randhawa, Head- Corporate Communications & Strategic Alliances, IFF and Mr Nikhil Bansal, Deputy Manager, IFF.

Microsoft
DECODING THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023
Understanding the need to be prepared for the Digi... Personal Data Protection Act, 2023
...day, 22th December 2023
1830 hrs - 2100 hrs
Regal, THE LaLiT, New Delhi
THE LaLiT
INDIA FUTURE FOUNDATION

IFF IN THE MEDIA

Kanishk Gaur, CEO, IFF, shared his insights on Deepfakes on DD National.

Kanishk Gaur, CEO, IFF, shared his insights on “Gemini”- Google’s most capable AI model on CNBC Awaaz.

Kanishk Gaur, CEO, IFF, shared his views on using AI Platforms for Financial Planning on ET NOW.

Kanishk Gaur, CEO, IFF, shared his views on using AI Platforms for Financial Planning on ET NOW Swadesh.

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