CYBER & DATA SECURITY SUMMIT 2025
STRENGTHENING DIGITAL RESILIENCE

ATTENDEES 300+

POWER-PACKED PANEL DISCUSSIONS 3

SPEAKERS 20+

e-BOOK LAUNCH

Girish Kathpalia

DIGNITARIES AT THE INAUGURATION OF CDS 2025

Dr. Pankaj Dixit

B. Shanker Jaiswal

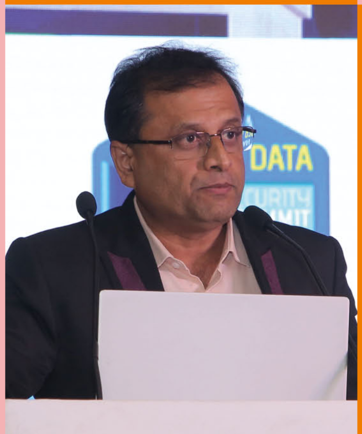
Prof. Kamaljeet Sandhu

Brijesh Singh, IPS

Dr. Pavan Duggal

Prof. Amlan Chakrabarti

Anuj Aggarwal


Dr. Harold D'costa

Ms. Deepa Ojha

Dr. Rakshit Tandon

Aman Thareja

Lee Nocon

Tarun Pratap Singh

Ram Vaidyanathan

Nakul Khandelwal

Rajaram Venkatesan

Akshay Garg

Dr. Deepak Kumar Sahu

CDS -Winners

PANEL DISCUSSION I: DATA PRIVACY: A TICKING TIME BOMB FOR THE INDUSTRY

Panel Discussion II: Mitigating Security Risks in Emerging Technologies

Panel Discussion Session III : From Risk to Resilience

Cyber & Data Security Summit 2025 Strengthening Digital Resilience

Cybersecurity is a shared responsibility, and through collaboration, businesses, corporations, CIOs, CTOs, and CISOs can foster a safer and more resilient digital world. With this fundamental principle in mind, the 9th edition of the Cyber & Data Security Summit 2025 was held in New Delhi. The event's theme, 'Recognizing Excellence in Digital Innovation', emphasized the need to build a secure, digital-first future where innovation and security are seamlessly integrated.

The summit focused on addressing the ever-evolving challenges posed by cyber threats and data security. It provided a platform for insightful discussions, keynote addresses, expert presentations, corporate insights, and valuable networking opportunities with cybersecurity and data privacy experts.

The event was graced by eminent dignitaries, including names like Shri B. Shanker Jaiswal, IPS, Joint CP (Operations & Licensing), Delhi Police, Brijesh Singh, IPS, ADGP Police & Principal Secretary to the Chief Minister, Government of Maharashtra, Justice Girish Kathpalia, Judge, Delhi High Court, Dr. Pavan Duggal, Advocate, Supreme Court of India, Lee Nocon, Co-Founder & CTO, Data Safeguard India, Prof. Kamaljeet Sandhu, University of New England, Australia, Prof. Amlan Chakrabarti, Director, A.K. Choudhury School of IT, University of Calcutta and Dr. Harold D'Costa, President, Cyber Security Corporation.

The event commenced with a welcome address by Dr. Deepak Kumar Sahu, Editor-in-Chief of VARINDIA. He spoke about the emerging trends in cybersecurity and artificial intelligence, highlighting India's significant strides in AI development. He mentioned the government's announcement of an indigenous Large Language Model (LLM) expected to be completed within ten months while also pointing out the rising cybersecurity threats. India ranks second globally in cyberattacks, with 95 organizations suffering data breaches in 2024, underscoring the need for enhanced security measures.

Dr. Pavan Duggal, Advocate, Supreme Court of India, delivered the inaugural address, engaging the audience with his insights into current cybersecurity trends and practices.

Followed by Shri B. Shanker Jaiswal, IPS, Joint CP (Operations & Licensing), Delhi Police, who provided an overview of cybercrime and digital security, discussing the future landscape of cybersecurity challenges and solutions.

Dr. Rakshit Tandon, Cybersecurity Evangelist & Risk Advisory Expert, spoke about AI's role in cybersecurity and how it could drive the next generation of cyberattacks.

Guest of Honour Brijesh Singh, IPS, ADGP & Principal Secretary to the Chief Minister of Maharashtra, delivered an inspiring address on cybersecurity and digital transformation, reinforcing the importance of proactive security measures.

While, Deepa Ojha, Manager, Privacy & Policy, DSCI, addressed data protection for a Digital India, then Dr. Pankaj Dikshit, CTO – GeM, Government of India, shared insights on securing IT systems against AI-generated threats. Given the event's focus on the current DPDPA, Anuj Aggarwal, Chairman of the Centre for Research on Cyber Crime & Cyber Law, leveraged the platform to provide insights into the challenges associated with DPDP implementation.

Prof. Kamaljeet Sandhu, University of New England, spoke on the challenges and opportunities AI presents for global cybersecurity leaders. Dr. Harold D'Costa, President of Cyber Security Corporation, provided the audience with an in-depth techno-legal perspective on mitigating cyber-attacks. He elaborated on the evolving nature of cyber threats, the legal challenges in prosecuting cybercriminals, and the need for stronger regulatory frameworks to enhance cybersecurity resilience.

Building on this, Hon'ble Justice Girish Kathpalia of the Delhi High Court delivered a compelling keynote address, taking the discussion to the next level. He outlined six critical use cases from the Indian judiciary where technology, particularly artificial intelligence (AI), could drive significant transformation. Justice Kathpalia emphasized that when applied responsibly, AI has the potential to revolutionize legal proceedings, streamline case management, and enhance judicial efficiency.

CDS 2025 had three interesting information loaded panel discussions. The first panel discussion, themed 'Data Privacy – A Ticking Time Bomb for the Industry', was moderated by Dr. Deepak Kumar Sahu and featured esteemed experts, including Sameer Mathur, Founder & CEO of S M Consulting; Sushant Mohapatra, Senior Lawyer at the Supreme Court of India; Shantanu Sahay, Partner at Anand and Anand; Major Subhendu Mahunta, Director of Financial Crime Prevention at FPL Technologies; Anil Kaushik, Founder & Vice Chairman of Cybercorp Ltd; and Mahi Gupta, Director of Privacy Strategy at Data Safeguard. The panel delved into pressing data privacy concerns, evolving legal frameworks, and effective strategies to mitigate associated risks.

The second panel discussion, on 'Mitigating Security Risks in Emerging Technologies', was moderated by Deepak Maheshwari, Senior Consultant at the Centre of Social & Economic Progress. It featured prominent industry leaders, including Pawan Chawla, CISO & DPPO of TATA AIA Life Insurance; Mayank Mehta, CISO of Bajaj Allianz Life Insurance; Kapil Madan, CISO & DPO of Max Healthcare; Amit Dhawan, CEO of Network Intelligence; Sujoy Brahmachari, CIO & CISO of Rosmerta Technologies Ltd.; and Manoj Srivastava, CIO of EaseMyTrip. The session explored the rising threats of cyber intrusions, emphasizing the critical need for advanced security frameworks to protect sensitive and business-critical information.

The third panel discussion, From Risk to Resilience, was moderated by Gyana Swain, Consulting Editor at VARINDIA, and brought together distinguished experts to discuss strategies for safeguarding critical assets while enabling innovation in an increasingly interconnected world. The panel featured Vijay Sethi, Chief Mentor & Digital Transformation Evangelist; Bharat B Anand, Group CIO & CTO of Connect Global; Bhaskar Rao, CISO of The Bharat Cooperative Bank Mumbai Ltd.; Khushbu Jain, Advocate at the Supreme Court of India & Founder of Ark Legal; Ritesh Kumar, Assistant Vice President at EXL; and Dr. Yusuf Hashmi, Group CISO at Jubilant Bhartia Group.

The event also had interesting Corporate Presentations from industry experts who provided valuable insights into various facets of cybersecurity and data protection initiatives.

Akshay Garg, Senior Presales & Business Manager at Varonis Systems, shared his expertise on data security and risk management, emphasizing the need for proactive threat mitigation strategies. Ram Vaidyanathan, Cybersecurity Evangelist at ManageEngine, explored the expanding role of artificial intelligence in cybersecurity beyond 2025, highlighting AI's potential in threat detection and response.

Nakul Khandelwal, Director of Product Management at Qualys, presented Risk Harmonics, offering a comprehensive analysis of enterprise cyber risk data and how organizations can leverage it for better risk management.

Rajaram Venkatesan, Geo Lead – India-South & Sri Lanka at SOTI, discussed next-generation mobile workforce management, focusing on security challenges and solutions for enterprises. Tarun Pratap Singh, Associate Vice President – Cyber Security Practice at Hitachi Systems India, outlined best practices in cybersecurity, stressing the importance of a multi-layered security approach.

Aman Thareja, Managing Director of Forcepoint India & South Asia, examined the latest security trends shaping the industry, providing a forward-looking perspective on emerging threats and defenses.

Lee Nocon, Co-Founder & CTO of Data Safeguard India, shared his expertise on data privacy, emphasizing the role of trusted partnerships in navigating the complexities of DPDPA compliance. He highlighted how businesses can effectively align with regulatory frameworks while ensuring robust data protection.

In the Tech Talk session, Prof. Amlan Chakrabarti, Professor and Director, A.K. Choudhury School of IT, University of Calcutta spoke on how to decode malicious cyrillic URLs, the threats that are powered by Deep Neural Networks. He went on to enlighten the audience on how cybercriminals use cyrillic-based URLs for phishing attacks.

The summit also featured the launch of the Technology Trends Handbook, an e-magazine compiling expert insights on top technology trends and forecasts. Next the event also witnessed the much-anticipated awards ceremony which recognized top security OEMs and vendors based on user feedback collected via the VARINDIA platform. Additionally, CDS 2025 celebrated the outstanding contributions of India's Top 10 Partners & VARs across various categories.

The Cyber & Data Security Summit 2025 successfully provided a vital platform for industry leaders, government officials, and cybersecurity experts to share insights and collaborate on strengthening digital resilience. The discussions underscored the importance of proactive security strategies, compliance, and innovation in navigating the complexities of today's digital landscape.

E-magazine : Technology Trends 2025 Handbook Unveiled

The Make in India initiative is accelerating India's ascent as a global manufacturing hub, strengthening IT hardware, semiconductors, and Fab industries. With the IT sector projected to reach US$ 350 billion by 2026, contributing 10% to GDP, India is solidifying its position as a global technology leader.

In line with this vision, VARINDIA has launched India's first Technology Trends Handbook e-Magazine, curated by Dr. Deepak Kumar Sahu, and his team to showcase emerging innovations and strategic insights. This compendium fosters industry collaboration and provides valuable intelligence to drive Make in India and Made for India enterprises. By bridging technological foresight with industrial growth, this initiative reinforces India's trajectory as a global powerhouse in technology and digital innovation.

The Role of Technology in Judiciary: Enhancing Efficiency and Trust

HON'BLE JUSTICE GIRISH KATHPALIA
DELHI HIGH COURT

"As a consumer of judicial technology, I want to share insights on what citizens expect from a modern justice system. One of the biggest challenges is the lack of continuity in leadership within IT departments of government institutions. Without dedicated experts who possess a missionary zeal for technological progress, innovation stagnates.

6 USE CASES OF INDIAN JUDICIARY SYSTEM

- A critical issue is the lack of synchronization between different departments. Many operate on incompatible systems, limiting the efficiency of technological solutions. The Interoperable Criminal Justice System (ICJS) is an attempt to bridge this gap, ensuring seamless communication between courts, police, and correctional facilities. Delays, such as bail orders taking a month to reach prisoners, create discontent. ICJS aims to prevent such issues, but its success hinges on system compatibility across institutions.
- Data protection is another pressing concern. Judicial records are stored on servers, yet we lack a legal framework to govern a secure, centralized repository. Delhi’s initiative to maintain a duplicate server in Madurai is a step forward, but a more comprehensive strategy is needed.
- Cybersecurity threats are also growing. A recent court hacking incident underscored the urgent need for stronger firewalls and AI-driven security protocols. The rise of deepfake technology poses additional risks, as manipulated evidence could threaten judicial integrity.
- AI-powered tools can streamline court proceedings. Automated transcription can save time, and AI-driven document summarization could help judges handling hundreds of cases daily. However, concerns about accuracy, ethical implications, and the irreplaceable role of human judgment must be considered.
- I believe that the market should start working on real-time vernacular-to-English text conversion for judges. However, local expressions pose challenges. Demeanor analysis is subjective, as judges are human. Still, Facial recognition could help assess truthfulness, though not with absolute certainty.
- Tech improves land records, voter verification, and docket management by ensuring transparency, reducing fraud, and improving efficiency.

Technology can also transform land record management, voter verification, and docket management by ensuring transparency, reducing fraud, and improving efficiency. While technology is a powerful enabler, it must be strategically implemented with strong safeguards. By addressing these challenges collaboratively, we can ensure that technological advancements strengthen the judiciary and uphold the cause of justice."

Harnessing AI: Balancing Innovation with Security

DR. PANKAJ DIXIT
CTO – GEM, GOVERNMENT OF INDIA

"The last two years have been transformative for AI, reshaping industries at an unprecedented pace. ChatGPT revolutionized the IT world, and now, with DeepSeek AI making waves, the evolution continues. AI agents are now streamlining business functions, from HR and document processing to financial analysis and security. Companies are actively seeking ways to maximize efficiency and ROI while navigating the inherent risks of AI adoption.

However, with great power comes great responsibility. AI’s potential for efficiency is matched by its potential for misuse. The rise of generative AI means threat actors can now automate cyberattacks at an alarming scale. What once took weeks to develop can now be executed in seconds. Malicious actors are leveraging AI to create advanced attack vectors, injecting scripts, breaching security systems, and exploiting vulnerabilities faster than ever. This necessitates a proactive defense strategy, ensuring enterprise security systems are equipped to counter AI-powered threats.

At GeM, we are integrating AI cautiously, ensuring that our data exposure remains minimal and secure. We have implemented stringent safeguards—ring-fencing queries, curating knowledge bases, and restricting AI interactions to public datasets. By scanning inputs and outputs for potential threats, we prevent AI-driven exploits from infiltrating our systems. Our security measures extend to increasing SOC capabilities, enhancing EPS thresholds, and reinforcing our defenses in collaboration with cloud partners.

Looking ahead, we plan to integrate AI into post-login functionalities, allowing users to query deeper databases while ensuring strict access controls. This will require careful structuring of data lakes and warehouses to maintain security. Additionally, we are enhancing our customer service through AI-driven multilingual chatbots, ticket automation, and IVR-based interactions, with seamless human-agent handovers.

AI is revolutionizing how we work, but it also demands heightened vigilance. By adopting a structured, security-first approach, we can harness its immense potential while safeguarding against emerging threats. The journey continues—one step at a time, with caution and innovation in balance."

GULF (Greed, Urgency, Love/Lust, Fear) leads to Digital Arrest

B. SHANKER JAISWAL
JT. CP (OPERATIONS & LICENSING) – DELHI POLICE

"Digital Arrest has gained significant traction recently, particularly in India, where cybercriminals have become more sophisticated in exploiting technology for fraud. While the term might sound futuristic, it refers to a very real and alarming phenomenon that has been increasingly affecting people. As technology advances, so do the tactics used by criminals.

I come from a law enforcement background with extensive experience in cybercrime research. Over the years, I've observed how criminals are exploiting technology faster than we can keep up. The concept of a "digital arrest" isn't just a sci-fi idea—it's part of a real-world scam. In these scams, criminals impersonate law enforcement officials, telling victims they're under investigation for illegal activities. They then demand large sums of money, often in cryptocurrency, to avoid being arrested. These scams are getting more sophisticated, and their impact is growing.

EXPLOITING EMOTIONAL TRIGGERS

One case involved an IIT Delhi graduate who was tricked into paying four lakh rupees after being told he was involved in illegal activity. The scammer, posing as a police officer, used a fake arrest warrant and manipulated the victim into transferring money. This money was then converted to cryptocurrency and sent overseas. Another case involved a doctor who was convinced to pay 5.6 crore rupees after a fake customs officer fabricated a story about fake drugs and passports.

So, why are people falling for these scams? After years of research in the Cyber Crime Division, I've identified key emotional triggers criminals exploit: Greed, Urgency, Love/Lust, and Fear (GULF). These emotions push victims to act quickly, often without thinking, which is exactly what the scammers want. The best way to protect ourselves is by being aware and cautious. We need to practice S.E.A.C.—Slow down, Evaluate, Act with Caution, and be sceptical. If something feels off, it probably is.

STAY INFORMED, STAY SAFE

Furthermore, with the rise of generative AI, criminals can create highly convincing fake identities, making these scams harder to spot. We must also push for stronger data protection laws, like the Digital Personal Data Protection (DPDP) Act, to safeguard our personal information. Finally, as technology evolves, so do the tactics of cybercriminals. By staying informed, cautious, and spreading awareness, we can collectively reduce the impact of these digital threats."

Strategic leadership and investment are crucial for AI's future in India

PROF. KAMALJEET SANDHU
UNIVERSITY OF NEW ENGLAND, ARMIDALE, NSW, AUSTRALIA

"As Director of the Australian government's AI Hub, I'm passionate about fostering global collaborations, particularly between Australia and India, as we navigate the complex and exciting landscape of artificial intelligence and cybersecurity. We stand at a critical juncture. AI is rapidly transforming our world, presenting both incredible opportunities and significant challenges. How we respond will define the coming decades. And that response hinges on two crucial elements: strong leadership and strategic investment.

LEADERSHIP DRIVES INNOVATION

Leadership is paramount. Without visionaries at the helm, we risk drifting aimlessly in this sea of technological change. Cybersecurity, fundamentally, is a human problem. Technology is just a tool; it's leadership that guides its ethical and effective use. And investment? That's the fuel that powers innovation. History is clear: from the rise of the internet to the dominance of today's tech giants, strategic investment has been the catalyst for groundbreaking advancements.

AI holds immense promise. Imagine cures for Alzheimer's, Parkinson's, cancer. This is the transformative potential we must unlock. But we can't let fear paralyze us. We need open minds, encouraging exploration and responsible development. We must learn from the past. Microsoft's mobile market misstep teaches us about the critical importance of timing. AI is at a similar crossroads. India, with its vast talent pool, can be an AI leader, but we need decisive action.

SEIZE THE AI MOMENT RESPONSIBLY

Cyber warfare is a real and growing threat. It's a multi-billion dollar industry with the power to cripple nations. We need robust cybersecurity strategies, advanced technology, and the best minds working on solutions. Cyberattacks are often unseen, undetected for years. We must be proactive. Cybercrime is another major concern, impacting everyone. While we can't ignore it, we can't let it stifle progress. We need safeguards, smart regulations, and widespread cybersecurity awareness.

The internet's evolution offers a valuable lesson. It started without a clear plan, growing organically. We should let the AI world develop similarly, while always prioritizing security. Security and leadership are two sides of the same coin. This is a massive opportunity for India. I see the passion here. We are the leaders of this technological revolution. Let's seize this moment and shape AI's future responsibly."

AI security risks exposing vulnerabilities in system integrity

BRIJESH SINGH, IPS
ADGP POLICE & PRINCIPAL SECRETARY TO CHIEF MINISTER, GOVT. OF MAHARASHTRA

"AI is undeniably powerful. It can create music, generate images, write text, solve complex problems, and even perform tasks traditionally done by humans. But as we embrace AI's capabilities, one question looms large: Is AI secure enough to handle such responsibility?

AI already plays a significant role in our lives. Facial recognition systems, for example, are used in law enforcement to determine who goes to jail or not. Autonomous vehicles make life-and-death decisions about the safety of passengers and pedestrians. With such influence over our daily lives, can we trust AI to be secure?

VULNERABILITIES IN AI SYSTEMS

Unfortunately, AI security is a serious concern. AI systems are vulnerable to various attacks that can compromise their integrity. For instance, early versions of GPT models had vulnerabilities, such as the "DAN (Do Anything Now)" prompt attack, which allowed users to bypass safety measures and prompt the AI to give harmful responses. Despite efforts to patch these weaknesses, AI models are still susceptible to similar attacks.

Moreover, AI systems can be manipulated to make poor or harmful decisions. Efforts to align AI models with human values sometimes result in overly cautious or flawed responses, which opens the door to uncensored models capable of answering anything. These models, though powerful, pose significant security risks. For example, autonomous driving systems like Tesla's can be misled by simple changes to road signs, like placing stickers on a stop sign. Similarly, facial recognition systems can be tricked by altering a person's appearance.

PROTECTING AI FROM EXPLOITS

AI models are also at risk of being stolen or poisoned. A "model inversion attack" could expose sensitive information, such as health data. Additionally, malicious actors could compromise the infrastructure supporting AI systems, injecting vulnerabilities or backdoors.

As AI replaces human workers in various fields, such as coding, the need to protect these systems becomes more urgent. Cybersecurity must evolve to address AI-specific risks, such as backdoors or hidden vulnerabilities that could be exploited in critical applications like banking or law enforcement.

To conclude, securing AI is essential. It's not just about protecting technology—it's about ensuring privacy, fairness, and security for everyone. We must continue innovating while safeguarding the future."

AI and cybersecurity must work in harmony for a secure future

DR. PAVAN DUGGAL
ADVOCATE - SUPREME COURT OF INDIA

"Let me take you back to ancient India, during King Ashoka's reign. Like Alexander, Ashoka expanded his empire with immense power. Two crucial figures led his kingdom: the King and the Senapati, or Commander-in-Chief. When they worked together, the empire thrived; if not, it faced downfall. In today's world, our empire is artificial intelligence. Here, AI is the King, while cybersecurity is the Commander-in-Chief. For our future to be secure, AI and cybersecurity must function in harmony. However, if cybersecurity fails, AI's growth and stability will be at risk, leading to challenges and threats in our increasingly digital world.

AI ADVANCEMENTS AND RISKS

The world has already seen the impact of AI in recent advancements. Tools like DeepFake and Qwen2.5 have reshaped productivity, but with them come significant risks. In the US, legislation is already being discussed to curb AI misuse, such as the "No DeepSeek on Government Devices Act." But we also face the challenge of AI-driven cybercrime, where fraud GPT is enabling cybercriminals to breach security systems undetected.

As we continue to develop AI, we must recognize the growing risks it brings, especially regarding privacy. For example, AI platforms often collect data from users without clear disclosure, creating vulnerabilities. Despite the promise of AI, we must remain cautious. The Indian ecosystem, often trusting by nature, must recognize that AI technologies aren't guaranteed to protect their data.

PREPARE, REGULATE, AND SAFEGUARD

AI is also complicating traditional cybercrime, where cybercriminals are empowered by AI algorithms to execute crimes on a global scale. The criminal element is no longer bound by geographical or legal boundaries. The task of tracing and prosecuting such crimes has become increasingly difficult.

Governments, including China and the EU, have already established frameworks to address AI's risks. In India, however, we are still lagging behind. We lack an AI-specific cybersecurity law and are yet to take meaningful steps toward creating a robust legal framework. As AI continues to evolve, we must urgently develop policies to ensure privacy, security, and accountability.

This is the age of AI, and the challenges it presents will only grow. It's time to prepare, to regulate, and to safeguard this new digital era with proactive, well-designed legal and cybersecurity frameworks."

Advancing AI and Cybersecurity through Research: A Focus on URL Classification

PROF. AMLAN CHAKRABARTI
PROFESSOR & DIRECTOR, UNIVERSITY OF CALCUTTA

"Today I will highlight the importance of research within our AI Hub, a strategic India-Australia partnership led by Professor Kamaljit and myself, dedicated to AI and cybersecurity. Also, I will discuss key research areas that are shaping the future of AI applications.

AI-driven applications are transforming both hardware and software by how data is used and processed, and much of this progress relies on foundational research. A significant area we are investigating is edge computing, which reduces latency by processing data closer to its source. However, edge computing introduces new security challenges, particularly in securing AI inference models and the data they process.

Another critical area is neuromorphic and in-memory computing, which offer promising advancements beyond traditional computing. Our ongoing research in these areas is making important strides.

I would like to share one of the exciting projects my Ph.D. student is working on, in collaboration with Professor Kamaljit, that involves identifying vulnerabilities in URL masking using different encoding techniques. This research aims to address security risks like phishing attacks that occur when URLs appear safe but are malicious.

A crucial aspect of this work involves the manipulation of URLs through UTF encoding. By using non-Latin characters that resemble Latin characters, attackers can deceive users into visiting fraudulent websites. Phishing attacks exploiting these vulnerabilities are on the rise and are expected to reach nearly 340,000 incidents by the end of 2024.

The advent of internationalized domain names (IDNs), which allow non-English characters in URLs, has compounded this issue. While this innovation benefits non-English speakers, it also opens new security risks.

Our research on URL classification, using models like Bi-directional LSTM, is one way we are tackling these challenges. The model has shown promising results and will soon be published for broader use. I encourage more to connect with the AI Hub to help build a robust ecosystem that addresses the security challenges emerging in AI and cybersecurity."

Navigating the Digital Personal Data Protection Act (DPDPA)

ANUJ AGGARWAL
CHAIRMAN, CENTRE FOR RESEARCH ON CYBER CRIME & CYBER LAW

"Today, instead of a formal presentation, I want to engage in an interactive discussion about the Digital Personal Data Protection Act (DPDPA). The law is now in place, with the draft rules already approved by the Home Ministry.

Let's start with a question: What does the DPDPA mean for Indian citizens? Many may think it applies only to Indian nationals, but that's a misconception. Unlike the GDPR, which is residency-based, the DPDPA applies to any transaction involving personal data within India, regardless of citizenship. This includes transactions by foreign nationals or even those that are free of charge.

A key feature of the DPDPA is its provisions on data transfer. While businesses may store data anywhere, the law remains applicable if the transaction involves India. The primary method of data collection under the DPDPA is consent, and this consent must be clear and easy to understand—no more lengthy agreements that are impossible to decipher.

Consent forms must be provided in at least 22 languages, but businesses should accommodate additional languages if needed. For instance, if you're operating in a diverse area, you might need to offer consent forms in Japanese, German, or other languages.

While consent is the primary method, data can also be collected for legitimate purposes, such as employment. However, this must be done with the principle of minimal data collection. For example, businesses cannot demand Aadhaar numbers unless specifically authorized by law, and Aadhaar cannot be used as proof of address or age.

The DPDPA also has provisions for minors. Any business wanting to process a child's data must obtain consent from the guardian, not the child, and verify the guardian's identity. The law is designed to be simple and effective, but businesses must understand their responsibilities and ensure their practices align with it. The DPDPA is here to stay, and compliance is key."

Cybersecurity & Digital Forensics: Mitigating Cyber Threats Before They Strike

DR. HAROLD D'COSTA
PRESIDENT CYBER SECURITY CORPORATION

"As someone with a forensic background, I can tell you that many of us trust platforms like WhatsApp for personal, professional, and confidential communication. Today, I've been hearing discussions around data privacy, the DPDP Act, and related concerns. To illustrate the point, let me share an example: my friend Rohit sent me an image on WhatsApp, but I received something entirely different. Now, people hesitate to share their numbers with me, as what you see isn't always what you get. This raises an important question: can we truly trust digital evidence?

This brings us to the need for effective cyber attack mitigation, which consists of three critical approaches:

Proactive Measures: Implementing firewalls, endpoint security, and threat intelligence to prevent attacks before they happen.

Reactive Measures: Establishing incident response plans, conducting forensic investigations, and taking legal action after an attack occurs.

Regulatory Compliance: Ensuring legal compliance, as many organizations fail to meet full compliance despite technical safeguards, leaving security gaps.

Many organizations focus on reactive measures rather than proactive ones. Let's take a look at some real-world breaches:

Cosmos Bank (2018): Rs. 94 crore lost due to weak cybersecurity measures.

IRCTC Data Leak: Personal data of 2 crore users exposed.

SpiceJet Ransomware Attack: Caused severe flight delays.

To mitigate cyber threats, organizations should use AI tools for phishing detection, implement immutable backups, adopt zero-trust access, and ensure continuous security posture management. With average breach losses of Rs. 12.8 crore and DPDP Act penalties up to Rs. 250 crore, proactive cybersecurity is essential, especially for critical infrastructure sectors.

Lastly, the example I showed earlier highlights a key issue with forensic admissibility under the Bharatiya Sakshya Adhiniyam 2023. If manipulated digital evidence is submitted in court, it could be mistaken for genuine evidence. This reinforces why forensic validation is critical before accepting digital content as truth."

Empowering Digital India: The Need for Strong Data Protection Frameworks

MS. DEEPA OJHA
MANAGER - PRIVACY & POLICY - DSCI

"As a policy expert in cybersecurity and data protection, I emphasize the critical role of data security in empowering individuals, businesses, and national security. India's regulatory framework is key to ensuring a secure digital ecosystem while promoting trust, compliance, and innovation.

WHY DATA PROTECTION MATTERS

With the rapid adoption of AI, IoT, and smart technologies, digitization has transformed industries but also increased cyber threats, data breaches, and privacy risks. A robust data protection framework is essential to balance business needs and individual rights.

KEY REASONS FOR DATA PROTECTION:

- Safeguarding Individual Privacy – Giving users control over their personal data.
- Building Business Trust – Compliance enhances consumer confidence.
- Enhancing National Security – Strengthening cybersecurity for critical infrastructure.

INDIA'S DATA PROTECTION LAWS

India's data protection journey evolved from the 2017 Puttaswamy judgment, which recognized privacy as a fundamental right, leading to the Digital Personal Data Protection Act (DPDPA) 2023. This law enforces purpose limitation, data minimization, and consent-driven processing. The Digital Personal Data Protection Act (DPDPA) 2023 aims to safeguard digital personal data while allowing lawful business operations. It ensures regulatory compliance by providing flexibility for data transfers and privacy innovations, enabling businesses to adapt to evolving data protection needs. Additionally, the law promotes industry-led cybersecurity practices, strengthening data security safeguards to mitigate risks. By balancing privacy protection and business interests, DPDPA 2023 fosters a secure, transparent, and trustworthy digital environment for individuals and enterprises alike.

By balancing privacy and business needs, the law fosters trust, transparency, and compliance in India's data-driven economy.

While DPDPA 2023 presents challenges—such as consent mechanisms, security obligations, and cross-border data flows—it also drives privacy innovation and cybersecurity advancements. At DSCI, we actively collaborate with government and industry stakeholders to create policy frameworks, cybersecurity guidelines, and training programs. Ensuring a secure digital ecosystem requires ongoing collaboration, innovation, and compliance."

Top prominent scams in 2024: fake stock trading, crypto investment scams and digital arrest

DR. RAKSHIT TANDON
CYBER SECURITY EVANGELIST AND RISK ADVISORY EXPERT

"According to recent data from the Indian Cybercrime Coordination Center (I4C), India reported 12 lakh (1.2 million) cybercrime complaints in the first nine months of 2024—equating to one cybercrime every minute. Financial losses from these scams amounted to a staggering ▯11,333 crores. Among the most significant cyber scams were fake stock trading, crypto investment frauds, and digital arrest scams, all contributing to massive financial damage. These scams exploited victims by manipulating trust and leveraging advanced cyber tactics.

Reflecting on the past, early cybercrimes primarily relied on social engineering. Scammers would call unsuspecting victims, posing as bank officials and tricking them into sharing OTPs—an infamous tactic originating from fraud hotspots like Jamtara. However, cybercriminals have since evolved significantly, adopting cutting-edge technology to enhance their deception. Even before companies could harness AI-driven cybersecurity, hackers had already begun using voice cloning, deepfakes, and AI-powered malware to exploit individuals. One of the most alarming threats today is the distribution of malicious APKs (Android Package Kits) through trusted contact attacks.

APKs function as advanced Trojans capable of stealing SMS data and banking credentials from infected devices. Hackers typically disguise these files as legitimate KYC verification updates from banks, convincing users to download and install them. Once installed, the malware grants hackers unauthorized access to sensitive information, leading to major financial losses. These APK-based cyberattacks remain a persistent challenge, as users often fail to recognize the deceptive nature of these files. Despite advancements in cybersecurity, India continues to struggle with preventing unauthorized APK installations, making it a pressing issue for law enforcement and tech security firms. Cybercrime has evolved from basic social engineering to AI-driven fraud, making awareness and proactive cybersecurity measures more critical than ever. As hackers grow more sophisticated, stronger security protocols, AI-enhanced fraud detection, and public awareness campaigns are essential to combat this escalating menace."

Navigating AI and Data Security: A Proactive Approach to Protecting Our Future

AMAN THAREJA
MD, FORCEPOINT INDIA & SA

"In today's rapidly evolving tech landscape, Artificial Intelligence (AI) is undoubtedly the fastest-growing technology, with a billion people expected to use it in just seven years. The impact on our lives will be profound, and it's crucial to integrate AI into every aspect of society, especially cybersecurity.

Cybercriminals are primarily after one thing: your data. With the global cost of a data breach averaging $4.5 million, organizations must prioritize data protection. In fact, cybercriminals are operating in a multi-trillion-dollar economy, underscoring the need for robust security measures.

Data protection regulations, such as DPDP, are evolving to ensure accountability throughout the data lifecycle—from collection to storage. Organizations must handle data responsibly, ensuring privacy and security, with strong systems in place to meet global standards.

At Forcepoint, we've developed an AI-powered Data Security Posture Management (DSPM) solution that autonomously identifies, classifies, and profiles data, helping organizations mitigate risks like access and retention vulnerabilities. Our AI leverages scalable, contextual decisions to improve efficiency and compliance, offering a dashboard that provides visibility and helps pinpoint high-risk areas.

In summary, a proactive, data-first approach is crucial for protecting sensitive information. Forcepoint is committed to delivering comprehensive data security, helping organizations adapt to new challenges and safeguard their most valuable assets."

Ensuring DPDP Compliance with Data Safeguard's ID Redact

LEE NOCON
CO-FOUNDER AND CTO, DATA SAFEGUARD

"Today, I'll focus on how Data Safeguard, dedicated to data privacy and synthetic fraud prevention since 2010 with strong presence in both the U.S. and India, helps businesses achieve DPDP compliance. While previous speakers have covered its key aspects, my focus is on practical solutions.

THE SHIFT FROM CYBERSECURITY TO DATA PRIVACY

For decades, investments have poured into cybersecurity, yet data privacy has been overlooked. With rising data breaches, the priority is no longer just preventing access but ensuring stolen data remains unusable. This shift is driving major investments in privacy and synthetic fraud prevention.

Smart devices collect vast amounts of personal data—over 500,000 PII elements per device. DPDP enforces strict privacy laws, mirroring global trends where fines surged from $8B to $16B in 2022. With enforcement expected in 12–18 months, businesses must act now.

ID REDACT: A COMPREHENSIVE DPDP SOLUTION

ID Redact is a comprehensive data privacy solution designed for global and Indian markets, integrating consent management, data discovery, access requests, redaction, privacy impact assessments, compliance audits, and real-time privacy monitoring. It enables businesses to manage cookie preferences, parental consent, and data processing while ensuring compliance with evolving regulations. With deployment in just two weeks and ROI in four, ID Redact prioritizes Privacy by Design, embedding robust security and compliance into every business process."

Beyond Passwords: The Future of Seamless Security

TARUN PRATAP SINGH

ASSOCIATE VP - CYBER SECURITY PRACTICE, HITACHI SYSTEMS INDIA

"In today's digital landscape, authentication is the foundation of security. Whether accessing a system, entering an office, or retrieving data, authentication plays a crucial role. However, traditional authentication methods, including passwords and two-factor authentication (2FA), are vulnerable. At Hitachi Systems India, we are pioneering a next-gen authentication platform that moves beyond passwords, ensuring seamless and secure access.

Today I will explore how advanced authentication methods—such as biometrics, behavioral analytics, and passwordless authentication—are transforming security frameworks. By integrating AI-driven adaptive authentication, organizations can detect anomalies in real-time and prevent fraudulent access. The rise of decentralized identity management and zero-trust architecture is further reshaping authentication, ensuring that security is continuous and context-aware rather than a one-time checkpoint.

However, as security tightens, user experience must not suffer. Striking the right balance is key to driving adoption and operational efficiency. We will discuss real-world case studies of organizations successfully implementing frictionless authentication while reducing risks and enhancing compliance with evolving regulations.

Looking ahead, innovations such as passkeys, blockchain-based identity verification, and continuous authentication will redefine digital trust. As cyber threats evolve, authentication must be dynamic, seamless, and intelligent.

Join us as we dive into the future of authentication, uncovering strategies to enhance security without compromising user convenience. The next era of authentication is here—are you ready to embrace it?"

Navigating AI and cybersecurity smartly in 2025 is critical

RAM VAIDYANATHAN

CYBERSECURITY EVANGELIST - MANAGEENGINE

"Today, we are at an interesting crossroads where artificial intelligence (AI) and cybersecurity intersect. On one hand, cybercriminals are leveraging AI to enhance their attacks, becoming more sophisticated and effective. On the other hand, as cybersecurity professionals, we need to use AI for all the good reasons to defend against these growing threats. The question we face is how we can harness its potential to strengthen defenses while managing the risks it brings. At Manage Engine, we develop a unified SIEM solution called Log360, designed to monitor and alert users when something goes wrong in their network.

A DOUBLE-EDGED SWORD

Cybercriminals are increasingly using AI to improve attacks. For example, AI-driven ransomware can target specific individuals or organizations, making the attack more personalized and harder to detect. It also powers malware that can adapt in real time to evade traditional defenses. Techniques like data poisoning or input manipulation allow attackers to bypass security systems. On the flip side, AI plays a vital role in defending against cyber threats. AI enables real-time threat detection, anomaly analysis, and faster forensic investigations. Integrating AI into identity security and access management reduces risk.

PREDICTIVE, PRESCRIPTIVE, AND REACTIVE

The three primary use cases for AI in cybersecurity are predictive, prescriptive, and reactive. Predictive AI helps with dynamic access control and proactive threat hunting. Prescriptive AI aids in anomaly detection, identifying unusual behaviour or phishing attacks. Reactive AI helps with post-breach analysis, learning from past incidents to prevent future attacks. In short, while AI introduces new challenges, it offers immense potential to enhance cybersecurity. We must leverage it to stay ahead of cybercriminals."

Qualys enables proactive risk management in cybersecurity

NAKUL KHANDELWAL

DIRECTOR, PRODUCT MANAGEMENT – QUALYS

"Digital transformation is expanding attack surfaces across hardware, software, IoT, and AI workloads, making the cybersecurity landscape more complex. Many organizations now use up to 70 cybersecurity products to address specific risks, but these tools often create security silos, making it harder to manage risks holistically. This is where a Risk Operation Center (ROC) becomes essential. Unlike traditional Security Operation Centers (SOC), which are reactive, a ROC focuses on proactive risk management. By aggregating indicators of exposure like vulnerabilities, misconfigurations, and identity risks across all assets, a ROC helps mitigate risks before they cause major security incidents.

SHAPING THE FUTURE OF RISK MANAGEMENT

The key to building an effective ROC is the right tools. Qualys' Enterprise True Risk Management platform is pivotal, unifying asset inventories, aggregating security findings, and offering a single view of risk posture. This enables organizations to measure, communicate, and act on risks in a timely manner, reducing silos and strengthening security. Additionally, the rise of AI and large language models (LLMs) introduces new risks. As LLMs become more widespread, many organizations lack visibility into the risks they pose, such as data leakage via prompt injection. Securing AI workloads is now a must.

STAY AHEAD OF FUTURE THREATS

Qualys offers solutions to detect vulnerabilities, prevent data theft, and protect AI systems. With increasing AI use, securing LLM workloads is critical. In conclusion, building a ROC and adopting a proactive risk management approach is more important than ever. With the right tools, like Qualys, organizations can manage the growing complexities of cybersecurity and stay ahead of emerging risks."

SOTI's secure, scalable solutions help businesses optimize their mobile operations

RAJARAM VENKATESAN
GEO LEAD- INDIA-SOUTH AND SRI LANKA, SOTI

"SOTI is a 30 years old and is headquartered at Mississauga, Canada. When you consider air travel, the moment you walk into the airport, you are checked in by the CISF people who scan your bags on all kinds of rugged industrial devices; we manage those devices. Then when you walk into the aircraft, the person who checks your boarding pass, then lets you in and again when you exit, there are devices which the service engineers use to do the inspections. These devices are also managed by us. So that is the spread of devices that we manage. In terms of growing our business, we always believe in investing back into the business. In India, we are headquartered in Gurgaon, and we also have a development center in Kochi. So half the strength of our global population will be out of India. We manage about 2.2 crore devices; some of our partners are the device partners as you need to have all the devices certified. We work very closely with them because it's not easy working with so many devices and to have SKUs of devices that could be made in the US or China. Unless you have those alliances ready, you cannot end up managing those devices single-handedly. Some of our customers could be anybody from the SMEs to the Fortune 100 companies. In India too, we have customers in BFSI, e-commerce, quick commerce, government, retail and so on. BFSI is a large vertical for us. In the drone industry, has a company called "SOTI Aerospace," which is a division of SOTI Inc. dedicated to advanced aerial drone and robotics research, essentially providing software solutions for managing and operating drones."

GenAI is a reality for enterprises today

AKSHAY GARG
SENIOR PRESALES & BUSINESS MANAGER – VARONIS SYSTEMS

"Generative AI is no longer a futuristic concept; it’s here, reshaping enterprise operations. Tools like Copilot and Gemini enhance productivity but also bring significant security risks, expanding the "blast radius" of accessible data and exacerbating vulnerabilities. Traditional, perimeter-based security strategies struggle to manage this evolving landscape. The core issue is a lack of focus on data itself. Many organizations don't know where sensitive data resides, who has access to it, or how it's being used. This knowledge gap, paired with GenAI's data-hungry nature, creates substantial risk.

PROACTIVE DSPM FOR GENAI SECURITY

A robust Data Security Posture Management (DSPM) strategy is essential. It should go beyond data discovery and classification, offering automated remediation for excessive permissions, identifying attack paths, and addressing identity misconfigurations. This proactive approach is key to securely adopting GenAI. Key DSPM capabilities include: comprehensive data discovery across all platforms, real-time risk assessment, automated remediation, and granular monitoring of data activity. GenAI governance is equally critical, ensuring visibility into tool usage, user prompts, file access, and conversations to prevent data exposure.

SECURING GENAI WITH VARONIS

Varonis Systems addresses these challenges with a platform that extends beyond basic DSPM, offering automated permission remediation, attack path analysis, and identity misconfiguration management. It provides the visibility and control organizations need to securely adopt GenAI. Varonis’ unified solution integrates DSPM and GenAI governance, empowering organizations to leverage AI’s benefits while minimizing risks. This shift from reactive breach response to proactive protection is the key to safely navigating GenAI's increasing presence."

CDS 2025: Calls for Action for a Secure, Resilient, and Digitally Empowered Future

DR. DEEPAK KUMAR SAHU
EDITOR-IN-CHIEF, VARINDIA

"The Cyber Data Security (CDS) Summit unites experts, thought leaders, and innovators from India and Singapore to shape the future of cybersecurity and digital transformation. Today, we honor the CIOs, CTOs, CISOs, and digital pioneers strengthening India’s cybersecurity landscape. Our Annual Cybersecurity and Rising Cybercrime Survey highlights India’s AI progress and growing cyber threats. The government’s push for an indigenous Large Language Model (LLM) within ten months marks a step toward AI independence. However, cyber risks are escalating rapidly.

India ranks second globally in cyberattacks, with 95% of organizations experiencing breaches in 2024. The financial, healthcare, government, and IT sectors remain prime targets. Cloud breaches are rising, affecting 67% of organizations due to misconfigurations and human errors. India accounts for 20% of global data breaches, often caused by unsecured APIs and weak encryption.

AI-driven cyber threats are a growing menace. 96% of deepfake content online is non-consensual, targeting women and public figures. India is among the top nations for AI-powered phishing and fraud attacks, with scammers using ChatGPT-like tools for sophisticated schemes. Generative AI is fueling phishing, voice cloning, and identity fraud, making detection harder.

To counter this, India has introduced the DPDP Act 2023 and CERT-In mandates for rapid cyber incident reporting. The National Cybersecurity Strategy 2024 emphasizes AI-driven security and cyber resilience. With 93% of IT leaders planning AI-driven security, the Indian cybersecurity market is set to reach $13.6 billion by 2027. The question remains—Is India prepared to combat these challenges? Now is the time to act. Let’s collaborate to build a secure, resilient, and AI-powered future."

TOP 10 OEMS IN THE CYBER SECURITY (PRODUCT & SOLUTIONS)

BEST COMPANY INTO CLOUD SECURITY SOLUTION -	QUALYS SECURITY TECHSERVICES PVT. LTD.
BEST DATA LOSS PREVENTION (DLP) PRODUCT -	FORCEPOINT SOFTWARE CONSULTING INDIA PRIVATE LIMITED
BEST UNIFIED ENDPOINT MANAGEMENT -	MANAGEENGINE, A DIVISION OF ZOHO CORPORATION
BEST THREAT INTELLIGENCE PLATFORM -	CYBLE SOLUTIONS PVT. LTD.
BEST SD-WAN SOLUTION PROVIDER -	FORTINET TECHNOLOGIES INDIA PVT. LTD.
BEST UNIFIED ENDPOINT MANAGEMENT -	SOTI INDIA PVT. LTD.
BEST COMPANY INTO NETWORK SECURITY -	CISCO SYSTEMS INDIA PVT. LTD.
BEST COMPANY INTO DATA SECURITY -	VARONIS SYSTEMS, INC
BEST COMPANY INTO DATA PRIVACY -	DATA SAFEGUARD INDIA PRIVATE LIMITED
BEST COMPANY INTO IT & OT SECURITY -	CHECKPOINT SOFTWARE TECHNOLOGIES INDIA PVT. LTD.

TOP 10 VARs IN THE CYBER SECURITY (PRODUCT & SOLUTIONS)

BEST VAR - CYBER SECURITY -	ADIT MICROSYS PVT. LTD.
BEST CLOUD SECURITY PARTNER -	INTENSITY GLOBAL TECHNOLOGIES PVT. LTD.
BEST MANAGED SECURITY SERVICE PROVIDER -	ALSTONIA CONSULTING LLP
BEST PARTNER INTO PROVIDING DATA PRIVACY SOLUTION-	HITACHI SYSTEMS INDIA PVT. LTD.
FASTEST GROWING CYBERSECURITY PARTNER -	ACPL SYSTEMS PVT. LTD.
BEST VALUE ADDED DISTRIBUTOR -	IVALUE INFOSOLUTIONS PVT. LTD.
BEST CRITICAL INFRASTRUCTURE SECURITY PARTNER -	VALUE POINT SYSTEMS PVT. LTD.
BEST NEXT GEN CYBER SECURITY -	BLACKBOX LTD.
EMERGING VAD IN INDIA -	FRUX TECHNOLOGIES PVT. LTD.
BEST DISTRIBUTOR INTO CYBER SECURITY -	RAH INFOTECH PVT. LTD.

CDS 2025 AUDIENCE

PANEL DISCUSSION I: DATA PRIVACY: A TICKING TIME BOMB FOR THE INDUSTRY

(FROM L TO R) MAHI GUPTA, DIRECTOR (PRIVACY STRATEGY) - DATA SAFEGUARD; SAMEER MATHUR, FOUNDER & CEO - S M CONSULTING; ANIL KAUSHIK, FOUNDER & VICE CHAIRMAN, CYBERCORP LTD; SHANTANU SAHAY, PARTNER- ANAND AND ANAND; MAJOR SUBHENDU MAHUNTA, DIRECTOR-FINANCIAL CRIME PREVENTION - FPL TECHNOLOGIES; SUSHANT MOHAPATRA, SR. LAWYER- SUPREME COURT OF INDIA AND DR. DEEPAK KUMAR SAHU, EDITOR-IN-CHIEF-VARINDIA

The first panel discussion for the day was on the topic - Data Privacy: A Ticking Time Bomb for the Industry and it was moderated by Dr. Deepak Kumar Sahu, Editor-in-chief-VARINDIA. The panelists who joined the session were Sameer Mathur, Founder & CEO - S M Consulting; Sushant Mohapatra, Sr. lawyer- Supreme Court of India; Shantanu Sahay, Partner- Anand and Anand; Major Subhendu Mahunta, Director-Financial Crime Prevention - FPL Technologies; Anil Kaushik, Founder & Vice Chairman, Cybercorp Ltd and Mahi Gupta, Director (Privacy Strategy) - Data Safeguard.

Talking about the critical challenges businesses face in handling personal data. Major Subhendu Mahunta mentioned the complexities of adapting to changing regulatory landscapes. “We are talking about the DPDP Act, the European Union’s GDPR laws and China again has its own regulations. So addressing all these challenges across different landscapes is a big constraint for every business. Many countries are adapting to these changing regulations, and how we address these challenges is a difficult task for the legal fraternity, because being non-compliant attracts regulatory penalties, including lawsuits. Secondly, any cross border transactions have its own ramifications. But in reality there is no standardization here. There are also complexities involved in taking the user consent, because not all the users are okay to share the data across the boundaries.”

Sameer Mathur explained, “Since I come from the Technology Advisory side and we conduct workshops on the DPDP Act compliance, there are 2-3 challenges that we see from the actual implementation side. One, the base of this law is the consent from the concerned data principal; taking and managing consent has become a very big challenge, especially for organizations where the number of data principals or number of PII holders is very, very large. So, whether it's a BFSI or ecommerce company or a logistic company or NBFC, managing consent is one of the biggest challenges. Another is about spreading awareness within the organization in terms of how do you convince people that this is not a cybersecurity issue, but a personal privacy issue. So we conduct an exercise called harm audit, where we try to convince the customer about the kind of harm that the loss or breach of personal data will incur.

Mahi Gupta further reiterated the point by adding that the biggest concern is to try understanding where does privacy end and what are the operational requirements for a business to conduct business. “I think the biggest challenge is that organizations think that with the advent of privacy laws, or cyber security regulation, doing business will be very tough. That's not what the intent of the regulation is. The regulation is saying that if you want to do certain things, just put certain guardrails around so that everybody's in a win-win situation. It's not like one side wins all and the other side loses everything. The balance that needs to be created is what the regulations demand.

On how he sees the current data privacy regulations evolving to emerging digital threats, Sushant Mohapatra said, “If we all remember, towards the end of 1999, there was this whole issue of Y2K that referred to the year 2000 and the potential computer issues that could have occurred when entering that year. It was also known as the millennium bug and it was said that everything will stop working, even banks for that matter. But slowly and efficiently we have migrated from that. So talking about this privacy law, these laws are already there in many areas, like CIBIL, the credit rating agency with which all our data is shared. But it is an integral part of the civil law itself of how the data should be protected. So instead of having fears about the implementation of this law, one should have an openness towards it because it is easy to comply with if you are aware of all the laws and rights.

Shantanu Sahay said, “One pertinent question as lawyers we always keep on asking ourselves is whether the law is caught up with the pace of technology. And the answer is no; there will always be some gaping lapses in terms of the way the technology has developed. Also, as a lawyer, and especially when I am focusing on issues of copyright violation and issues of other legal matters, I am confronted with the situation of whether the law in cases of a violation and also in a situation of Regulation, is in the position to deal with these issues with the right technology process. But I am 100% positive today, that so far as the substantive law is concerned in India, we are pretty much certain that we have the structure to deal with these lapses.”

On how organizations ensure ethical and secure data use, Anil Kaushik said, “The ownership of the data is with the creator of the data or the data principal, which is the bottom line. Secondly, no data privacy can go without the liabilities attached to that. So liabilities will be increased, they will be there and those could be even more stringent in the future. The lapses which I could see in the system is the absence of provision for keeping the data, of how to store the data and where to store the critical data.”

PANEL DISCUSSION II: MITIGATING SECURITY RISKS IN EMERGING TECHNOLOGIES

(FROM L TO R) PAWAN CHAWLA, CISO & DPPO- TATA AIA LIFE INSURANCE; MAYANK MEHTA, CISO- BAJAJ ALLIANZ LIFE INSURANCE; ROHIT RAMAN, MANAGING PARTNER & APAC HEAD – ETEK INTERNATIONAL; DEEPAK MAHESHWARI, SR. CONSULTANT- CENTRE OF SOCIAL & ECONOMIC PROGRESS; AMIT DHAWAN, CEO - NETWORK INTELLIGENCE; SUJOY BRAHMACHARI, CIO & CISO- ROSMERTA TECHNOLOGIES LTD. AND MANOJ SRIVASTAVA, CIO- EASEMYTRIP

The second panel discussion for the day was titled - Mitigating Security Risks in Emerging Technologies and it was moderated by Deepak Maheshwari, Sr. Consultant- Centre of Social & Economic Progress. The panelists for this session included Pawan Chawla, CISO & DPPO- TATA AIA Life Insurance; Mayank Mehta, CISO- Bajaj Allianz Life Insurance; Rohit Raman, Managing Partner & APAC Head – ETEK International; Amit Dhawan, CEO - Network Intelligence; Sujoy Brahmachari, CIO & CISO- Rosmerta Technologies Ltd. and Manoj Srivastava, CIO- EaseMyTrip. The session delved on how with the surge of cyber intrusions over the past decade that causes data breaches, disruptions, and financial losses, highlights the urgent need for strong cybersecurity to protect critical information and infrastructure.

Deepak Maheshwari opened the discussion by saying that while threat actors (Chor) and defenders (Police) all use the same technologies and tools, but it is just a matter of who is ahead in the game. “But when it comes to the use of Gen AI, or AI in general, the speed at which things are happening, the scale at which things are happening, that's something which becomes extremely important for us to look at.”

On how his organization ensures cybersecurity and data protection while deploying new technologies, Pawan Chawla said that both cyber security and data protection go hand in hand. “But as an organization, we can't play around with multiple tools. We have a limited set of tools with which we need to work upon. Hacking has become an organized crime and I would say the hacking industry is much more regulated than any other industry. Data is not only the fuel for the organization, but it is the real-time fuel. The market is changing so fast that you need to have real time data to change your dynamics as well. So when it comes to adopting a new technology, it is important to identify the vulnerabilities before adopting it. It should fit within your environment.”

Speaking about some of the ambiguities that still exist in the present system, Mayank Mehta stated that while in certain cases it required six hours to report an incident, the DPDP Act draft rules says that any breach that takes place needs to be reported within 72 hours. “Since in the insurance industry, we happen to report any such incidence to IRDA, will this framework fit into these newly set rules. All these things need to be unified so that organizations can take the critical approach. Most of the time, because of this ambiguous nature, organizations who are ethical will always try to go according to the rules while some will take their own call.”

While explaining how his organization ensures data protection, Sujoy Brahmachari said that there should be a right balance between an organizations’ application as well as UX, which is customer experience and the security of the application product. “So it's a combination of both. Cyber security and data security should not be an after-thought and it should be implemented from Day 1 after testing it properly. You need to have a good, robust mobility application which every user can use. The ease of use is very important. And apart from that, you need to have a good access control and authentication mechanism as well as a monitoring mechanism, so that both things go hand in hand.”

Manoj Srivastava said that his company has been into travel technology for the last 20 years. “Today, talking about data protection or cyber security, we have to go through a lot of due diligence since we deal with a lot of customer data. Firstly, we need to look into compliance by sharing all the necessary documents. Next is the technical part, when we have a lot of regression testing on our software before making it live. Before going live, we also take care of data protection so that it does not go into the wrong hands. Also, we are connected in real time and so there is no chance for error.”

Amit Dhawan said that on a lighter note, the threats will never be technical, but it comes out of the human firewall. “You can have a billion-dollar equipment, but then somebody will create a server or an MTP server and leak out data. So the human firewall element is one of the most important things. We can talk about users who are using it, but the security folks themselves are at fault most of the time. And I keep repeating very often that a fool behind a tool is always a fool. You can get any amount of infrastructure in place, but if you do not have the right capability to manage it, it is going to fail.”

Talking about the unique challenges and opportunities in the healthcare sector, Rohit Raman said, “Being a cybersecurity specialist, I understand that with the use of AI and digitalization in the health sector, there has been a lot of improvement. At the same time, we also see that it is bringing out a lot of good things in terms of informed decisions by the health practitioners, whereby ultimately, the benefit goes to the patient in terms of high rate of success in treatments. AI and database information will help you diagnose the problem in a much better manner. But the biggest challenge, however, is the integration. There is no formal standardization of data in the health sector, at least in India.”

PANEL DISCUSSION SESSION III : FROM RISK TO RESILIENCE

(FROM L TO R) GYANA SWAIN, CONSULTING EDITOR- VARINDIA; VIJAY SETHI, CHIEF MENTOR- DIGITAL TRANSFORMATION AND SUSTAINABILITY EVANGELIST; KHUSHBU JAIN, ADVOCATE- SUPREME COURT OF INDIA & FOUNDER - ARK LEGAL; BHAVESH KUMAR, CHIEF INFORMATION SECURITY OFFICER & DPO – SK FINANCE LIMITED; BHASKAR RAO, CISO - THE BHARAT COOPERATIVE BANK MUMBAI LTD. AND BHARAT B ANAND, GROUP CHIEF INFORMATION & TECHNOLOGY OFFICER- CONNECT GLOBAL

The third panel discussion session entitled - From Risk to Resilience was moderated by Gyana Swain, Consulting Editor- VARINDIA. The panelists joining this session were Vijay Sethi, Chief Mentor- Digital transformation and sustainability evangelist; Khushbu Jain, Advocate- Supreme Court of India & Founder - Ark Legal; Bhaskar Rao, CISO - The Bharat Cooperative Bank Mumbai Ltd.; Bhavesh Kumar, Chief Information Security Officer & DPO – SK Finance Limited and Bharat B Anand, Group Chief Information & Technology Officer- Connect Global.

Gyana Swain began the discussion by citing data from RBI (Reserve Bank of India) which says that in the last two decades, there have been a loss of more than $20 billion through cyber-attacks. “Another report says that more than 2500 cyber attacks happen in the BFSI sector every week, which is also hard to believe since daily transactions are close to Rs 18 crores in the country alone, against which this figure is quite minuscule.”

Speaking about the biggest security challenges in 2025, Vijay Sethi said that while AI is increasing a lot, the AI-based threats are also increasing at the same pace. “Rather than just the traditional threats that have been there, AI would be now used more to exploit the vulnerability. Also all the phishing attacks and the ransomware attacks, which have been there for quite some time now, would become much more sophisticated because of AI. I am convinced that the attackers know more about AI than the defenders or any organization. The second major risk that I see is the third party risk. The BFSI with its huge number of stakeholders become a huge entry point for threats. So while one can get into zero trust or any other security measures, the reality is most of the organizations are not working on that.”

Khushbu Jain said that while talking about the threat that comes with the use of AI, we also have to look into the aspect of what are the vulnerabilities when we are using AI. “It is good to inculcate AI in your organization when it comes to fighting cyber crimes or when it comes to creating the ecosystem for cybersecurity, but by utilizing that you have to have a lot of things in mind. Today you talk about privacy by design, but it's very difficult to implement privacy by design. And that's where you need to understand the biasness, or how vulnerable those AI things would be, or what all data sets are you utilizing for building different AI models. What are the laws prevalent now; the DPDP Act is there, but apart from this, GDPR and a lot of other privacy laws are existent worldwide. So you will have to be mindful of that. You will have to see that the company who is providing you with data, is there a proper consent for that mechanism? If you don't have that consent, tomorrow you will land up in litigation and this will create difficulties for you.”

Agreeing with both the panelists, Bhaskar Rao said, “We are a cooperative bank, and we are more dependent on the third party. The supply chain, I think, happens to be one of the most vulnerable spots as most of us are dependent on the services provided by the third party. If you recall an incident 4- 5 months back, there was an attack on one of the prominent banking technology providers and this led to 300 banks being cut off and experiencing a major outage. The hackers have come to realize the dependency of the banks on a central repository and they target that for stealing data, eventually disrupting the entire supply chain and the entire banking functionality in the process.”

Bhavesh Kumar said that while talking about cyber risk or compliance risk, the compliance or regulatory requirement is laid down by a different regulator to protect the stakeholders from cyber and fraud risk. “So if we are protecting or implementing effective controls, automatically we will comply with the compliance. In BFSI, since we are a fiduciary for our customer as we have in possession the confidential or personal information of our individual customers, and so to address the risk the first thing we should do is to fix our basics. So when we say basics, we must implement effective technology, processes and effective awareness mechanisms in our organization to disseminate each and every regulatory compliance related information and cyber related information.”

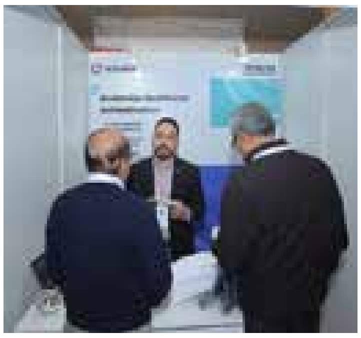
Bharat B Anand “So we are name-dropping AI these days. It's just like the Cloud in early 2000 and digital in 2010-12 onwards and now it's the AI. But AI is both an opportunity and a challenge, and we as a technologist, as well as the business owners or the vertical head, we need to take care of both the aspects. As much as you need to shore up your fences using whatever you can, it is just not about the devices you have put but it's more about what policies, what SOPs, what frameworks you put in practice. It is also about very close monitoring which you need to do, and auditing those monitors which you have put up besides creating awareness within the organization.”

CDS 2025 EVENT AT A GLANCE

ICICI BANK

DATA SAFEGUARD INDIA

MANAGEENGINE



1KOSMOS | HITACHI

FORCEPOINT | IVALUE

FRUX TECHNOLOGIES

HERITAGE CYBER WORLD

QUALYS

SOTI

PICUS | REGENT

LUCKY DRAW WINNER

LUCKY DRAW WINNER

LUCKY DRAW WINNER

LUCKY DRAW WINNER

LUCKY DRAW WINNER

SPONSORS

PARTNERS

SUPPORTED BY

AI HUB

POWERED BY

VARONIS

PRINCIPAL PARTNER

SOTI

PLATINUM PARTNER

1KOSMOS | HITACHI Inspire the Next

PRIVACY PARTNER

datasafeguard Privacy Management

GOLD PARTNERS

ManageEngine

Qualys.

Forcepoint | iVALUE

NETWORKING PARTNER

Sandyne Technologies

EXHIBIT PARTNERS

HERITAGE CYBERWORLD LLP

FRUX

PICUS | Regent

SUPPORTING PARTNERS

ISODA Infotech Software Dealers Association

PCAIT