Digital Turbulence — Navigating Law Amidst Bytes

In an age propelled by swift technological progress, the ominous rise of cybercrime emerges as an unparalleled global conundrum. India, accounting for over 13% of cyberattacks worldwide, is at the forefront of this battle.

By Minu Sirsalewala

In this exclusive interview, **Aniruddha Majumdar,** Senior Member of the TMT and Cybersecurity Practice at Nishith Desai Associates, in conversation with **Minu Sirsalewala,** Executive Editor – Special Projects, provides invaluable insights into India's current cybersecurity landscape. He delves into the legal framework's evolution, critical gaps, international collaboration, and the delicate balance between fostering innovation and imposing regulations.

With the surge in cybercrime globally, how do you assess India's current cybersecurity landscape, and what are the key challenges that need urgent attention?

India is subject to more than 13% of cyberattacks globally, and that is a disproportionate and concerning number. India's current cybersecurity landscape has improved significantly over the past few decades. However, a lot of key challenges still remain. News of cyberattacks and breaches affecting Government and private organisations are increasingly common. The key challenge remains that of awareness – of both the kind of attacks that an organisation could be subjected to, and the risks that this could pose. The smaller businesses and organisations, especially, need to make cybersecurity second nature, because even one successful attack can prove very costly.

ANIRUDDHA MAJUMDAR
Senior Member, TMT and Cybersecurity Practice,
Nishith Desai Associates

Given the dynamic nature of cyber threats, how has India's legal framework evolved over the years to address emerging challenges? Are there specific legislative trends that stand out in enhancing cybersecurity laws?

The Government has been highly active in this space, and has emphasised on numerous occasions that its vision is to ensure a safe and trusted internet for digital citizens. The CERT-In Directions of 2022 were a major step in this direction, and contains more strict obligations on all kinds of entities for cybersecurity matters. The DPDPA also contains notification and security requirements for personal data breaches. Other sectoral regulators have also picked up on cybersecurity requirements including RBI and SEBI, which is great, given the sensitive sectors that these authorities oversee. Overall, there has been a conscious move towards obligating organisations to move towards better cybersecurity measures as well as informing regulators regarding incidents – so that at least the Government has visibility on the nature of attacks.

In your analysis, what critical gaps do you identify in India's current cybersecurity laws, and what are the main challenges in their effective enforcement? Are there specific areas that require immediate attention from policymakers?

When it comes to the CERT-In Directions, 2022, a few provisions are quite vague and have led to regulatory uncertainty. This has been the case despite FAQs being issued. There is also a view among industry players that some obligations are too strict and difficult to comply with. Regulatory uncertainty and over-regulation can defeat the purpose of a law since these encourage non-compliance. It is important that policymakers engage with the industry on a periodic basis to understand pain points and how to streamline cybersecurity laws.

How can India's legal framework facilitate international collaboration against cross-border cyber threats? Any best practices from other jurisdictions to adopt? Changes in strategies in response to recent global cyber incidents?

India has signed numerous bilateral agreements with other countries pertaining to cooperation over the investigation and mitigation of cyber threats. Given the cross-border nature of cyber threats, such cooperation becomes inevitable. Some of the key treaties have been with US, UK and Japan. The CERT-In also coordinates with its counterparts across the globe in sharing information on cyber threats – which enables better preparedness for both countries. There has also been a notable increase in state-sponsored cyberattacks and alliances are forming between countries to enhance collective security against such attacks which can be quite sophisticated and damaging.

Considering the rapid evolution of technology and cyber threats, what recommendations do you propose for ensuring that India's legal mechanisms stay ahead in addressing future challenges in the realm of cybersecurity? Are there specific areas of law that require proactive amendments or enhancements? For example, deepfake threats & frauds, generative AI frauds etc.

Emerging technology always poses a challenge when it comes to regulation. Deepfakes and AI, in general, have considerable potential to harm users and even organisations. In such a case, it may be too risky to play catch-up. To enhance the pace of regulations, it is important that the Government works collaboratively with developers of these technologies on a continuous basis to keep abreast of what is coming up next.

In the technology and media sectors, innovation is rapid. How do you see the balance between fostering innovation and imposing regulations in the cybersecurity domain? Are there instances where regulatory measures might stifle innovation, or vice versa?

Indeed, regulations are typically slow-paced. We have seen numerous examples of laws lagging behind emerging technology over the years. India's DPDPA has also been criticised at times for coming in too late. On the other side, it can also be argued that fast-paced regulation is often reactionary, and ineffective. This leaves regulators in a perpetual dilemma of when to regulate. Collaboration and dialogues with the industry can be helpful here to understand which are the most pressing issues which need regulatory attention urgently. Even otherwise, the industry needs to take it upon itself to ensure that it innovates responsibly, regardless of any regulations in place. This will help build trust with consumers, which is better from a demand perspective as well. Additionally, this creates goodwill with the Government and the regulators can focus on harms which are not being addressed by the market.

minus@cybermedia.co.in