Is India ready for AI-Powered cyber war?

In conversation with e4m's Brij Pahwa, Quick Heal CMO Sudhanshu Tripathi discusses the rising tide of AI-driven cyber threats, how brands can turn cybersecurity into a competitive advantage and more

by **Brij Pahwa**

Published: Apr 1, 2025 12:29 PM | 9 MIN READ

In conversation with e4m, Sudhanshu Tripathi, CMO at Quick Heal, sheds light on the rising tide of AI-driven cyber threats, with India witnessing over 369 million incidents. He discusses how brands can turn cybersecurity into a competitive advantage, the role of AI in safeguarding businesses, and what lies ahead for digital security in an era of deepfakes and fintech fraud.

Q1. How can brands turn cybersecurity from a liability into a competitive advantage in today's digital economy?

The insights from the India Cyber Threat Report 2025 reveal that malware detections are growing at an alarming rate, with over 369 million incidents recorded across India. In today's digital economy, cybersecurity is no longer optional—it's the backbone of customer trust and business resilience. Without robust security measures, brands risk devastating breaches that can cripple operations, damage reputations, and result in massive financial losses.

At Seqrite Labs—India's largest malware analysis center, our research highlights how proactive tools like Seqrite Malware Analysis Platform (SMAP) and Seqrite Threat Intel (STI) empower CISOs to prevent losses, safeguard operations, and turn cybersecurity from a liability into a competitive advantage by driving trust and measurable business outcomes.

Moreover, brands with a mature cybersecurity posture not only mitigate risks but also perform better in ESG assessments, which are increasingly influencing investment decisions. A strong cybersecurity framework enhances investor confidence, boosts brand valuation, and attracts partners and talent seeking to align with resilient and responsible organizations.

By taking a comprehensive approach to cybersecurity, brands can strengthen their operational security while positioning themselves ahead of the competition in today's evolving digital landscape.

Q2. As AI-driven cyber threats become more sophisticated, do you think businesses are overestimating their security preparedness? What's the biggest blind spot?

Absolutely, businesses often overestimate their security preparedness, especially as AI-driven cyber threats become increasingly sophisticated. The biggest blind spot is reliance on outdated tools that can't keep pace with evolving attack vectors. At Quick Heal and Seqrite, we've been AI-native from the start, with patented technology like GoDeep.AI powering our advanced tech stack. As the only cybersecurity firm from India to be a member of US AISIC, we're actively shaping the global narrative on AI in cybersecurity.

Another critical blind spot is the lack of cybersecurity awareness among employees. With AI-driven phishing and social engineering tactics becoming more convincing, human error remains a major point of exploitation. Investing in cybersecurity awareness programs and regular training is essential to building a resilient security posture.

Organizations must harness AI's capabilities to defend against AI-powered attacks. By adopting AI-driven cybersecurity solutions, businesses can stay ahead of sophisticated threats, safeguarding their operations, reputation, and bottom line—while turning cybersecurity into a strategic advantage.

Q3. India is experiencing a fintech boom, yet digital fraud is skyrocketing. Do you think regulators and companies are doing enough to protect users? What more needs to be done?

I commend the regulators for their proactive efforts in a rapidly evolving ecosystem. They are undoubtedly making significant strides in combating digital fraud. The introduction of the DPDP Act marks a crucial step toward safeguarding personal data and strengthening privacy and security standards. The recently released draft DPDP Rules mandate clear user consent before data processing and impose stringent penalties for non- compliance—helping deter data breaches and misuse. Additionally, the RBI's initiative to introduce exclusive domain names for banks and financial services, such as '.bank.in' and '.fin.in', is a positive move toward reducing phishing scams and enhancing online credibility. However, these measures alone are not enough.

To further combat digital fraud, businesses must invest in advanced AI and ML technologies to detect threats in real time and collaborate more closely with regulators to enhance cybersecurity standards and awareness. A multi-pronged approach is essential—implementing Endpoint Detection and Response (EDR) solutions, leveraging real-time threat intelligence for proactive fraud identification, and conducting regular security audits and awareness training for employees and customers. By combining these efforts with regulatory initiatives, we can create a more secure digital ecosystem for users.

From a consumer perspective, awareness alone is no longer sufficient. In the fast-paced fintech world, users need robust, real-time protection. That's where AntiFraud.AI makes a difference. As India's first AI-driven fraud prevention solution, it proactively stops threats before they cause harm—unlike conventional solutions that react after the damage is done.

Building a secure digital ecosystem requires a multi-faceted approach—leveraging advanced technology, collaborating with regulators, and empowering consumers with solutions like AntiFraud.AI to stay ahead of evolving threats.

Q4. With deepfakes and AI-generated scams on the rise, how should brands protect themselves and their consumers from identity fraud and misinformation?

Deepfakes and AI-generated scams represent a new frontier in cybercrime. To combat these threats, it is important to deploy advanced AI-driven tools capable of detecting manipulated content in real time. Seqrite's Endpoint Detection and Response (EDR) solution employs behavioral analysis and deep learning through its GoDeep.AI engine to identify anomalous patterns in network traffic and file operations that might indicate deepfake propagation or synthetic media manipulation. The integrated File Sandboxing feature analyzes suspicious files in isolated environments, effectively detecting AI-generated malware payloads often embedded in deepfake delivery mechanisms. While leveraging these solutions, brands should also implement multi-factor authentication (MFA) across all consumer-facing platforms. At the same time, consumer education programs about recognizing phishing attempts and verifying communications through official channels remain critical. By combining these technical safeguards with user awareness initiatives, brands can mitigate risks while maintaining trust in an era of synthetic media proliferation.

Q5. First-party data is becoming the new gold as third-party cookies phase out. How should brands rethink their marketing strategies in a post-cookie world?

In the post-cookie era, security isn't just a compliance checkbox—it's a growth enabler. The shift to first-party data requires strategies where security and trust become competitive advantages. At Seqrite, we facilitate this through one of our advanced solutions, leveraging behavioral analytics and real-time threat detection to safeguard customer data ecosystems. Our Data Loss Prevention (DLP) tools utilize AES-256 encryption across stored and transmitted data, ensuring compliance with India's DPDP Act while strengthening consumer confidence. We also support RBI's domain authentication protocols to validate legitimate communication channels, mitigating phishing risks.

Brands have developed an insatiable hunger for data, voraciously consuming consumer information. However, with the implementation of the DPDP Act, it's time for brands to pause and reassess. They must evaluate the necessity of customer data based on core business needs and strike a sustainable balance between data collection and respecting consumer privacy.

Q6. Social commerce and influencer-driven marketing are reshaping consumer behavior. Do you think traditional ad-driven performance marketing will become obsolete?

While social commerce and influencer marketing are gaining traction due to their personalized nature, traditional ad-driven performance marketing remains crucial for achieving broad reach and brand awareness. The key is integration rather than replacement. Brands that combine the credibility of influencer-driven content with the precision of ad-driven performance marketing can maximize impact. By leveraging data insights from ad campaigns to refine influencer strategies, businesses can create a holistic approach that drives both reach and conversions.

Rather than becoming obsolete, ad-driven performance marketing will evolve to complement newer strategies— helping brands stay agile and relevant in a rapidly changing digital landscape.

Q7. Voice search, AR, and immersive experiences are redefining digital marketing. What's the next big technological shift that CMOs should prepare for?

The next major shift, in my opinion, will involve AI-powered personalization within immersive environments like the metaverse and augmented reality (AR) platforms. These technologies will enable hyper-targeted campaigns based on real-time behavioral data. However, as highlighted in our India Cyber Threat Report 2025, emerging technologies also introduce new vulnerabilities, such as insecure APIs or tampered IoT devices within AR ecosystems. CMOs must collaborate closely with CISOs and DPOs to secure and optimize these platforms using solutions like Seqrite's SMAP and EPS for comprehensive protection against evolving threats.

Another critical aspect will be upskilling marketing teams to effectively integrate and leverage these new technologies. Ensuring that teams maintain their marketing expertise while unlocking greater value through the optimal use of next-gen tools and media will be crucial for staying ahead in the digital landscape.

Q8. If you had an unlimited marketing budget for Quick Heal, what's one bold, unconventional campaign you'd execute to make cybersecurity mainstream and viral?

At Seqrite, we believe cybersecurity awareness can't be driven by just one campaign or channel. It demands a multi-dimensional approach. We are already investing significantly across social media platforms to promote products like AntiFraud.AI, alongside strategic placements in TV, print, and retail environments. Influencer marketing and active participation in global events further amplify our reach and credibility.

If resources were unlimited, one morning, QR codes would mysteriously appear at government offices, railway stations, airports, and iconic public buildings across India, urging people to scan and sign up for "Cyber Safety as a Fundamental Right." As curiosity peaks, millions of citizens scan the code and land on a pledge demanding that the government recognize cybersecurity as a basic right—ensuring free baseline protection, digital safety education in schools, stricter cybercrime laws, and peace of mind while navigating the digital world.

The movement quickly gains momentum with a staged “Cyber Blackout” stunt on social media, simulating the chaos of cybercriminals taking control—creating a sense of urgency and awareness. Influential voices from celebrities, tech leaders, and digital advocates amplify the message, while policy advocacy efforts push for India’s first Digital Safety Law. Backed by mass public engagement, this bold campaign transforms cybersecurity into a national movement, making Cyber Safety a Fundamental Right for every Indian.