Mayl 10, 2026 Volume 14

PRAGYA CONSULTING

SUSTAINABLE SOCIAL SENSIBLE

India's First Magazine dedicated to MSMEs

BizIgnite

POWERING INDIA'S MSME REVOLUTION

IN COLLABORATION WITH: ni-msme®

MSME DIGITAL MASTERY

CYBERSECURITY & AI

UNDERSTANDING CUSTOMER PSYCHOLOGY

CYBERSECURITY & AI: THE NEW SURVIVAL TOOLKIT FOR MSMEs

AI Focus

As Indian MSMEs rapidly embrace digital payments, cloud platforms, online banking, GST systems, e-commerce, and AI-driven tools, cybersecurity is no longer a concern limited to large corporations—it has become a critical business survival issue for every enterprise, regardless of size.

From phishing scams and payment fraud to ransomware attacks and data breaches, cyber threats today are targeting the weakest digital defenses, and MSMEs are increasingly becoming prime targets.

In an interconnected economy, a single cyber incident can disrupt operations, damage customer trust, and lead to severe financial losses.

At the same time, the rise of affordable **AI-powered cyber-security solutions** is giving MSMEs an unprecedented opportunity to shift from reactive protection to intelligent, predictive security. Tools that once seemed accessible only to large enterprises are now available to small businesses at practical costs, enabling them to automate threat detection, secure transactions, monitor suspicious activity, and strengthen operational resilience.

In this exclusive conversation with BizIgnite, **Mr. Tarun Wig, Co-founder & CEO, Innefu Labs explains why cybersecurity is now a business-critical priority for Indian MSMEs—and how AI-powered tools can help small businesses stay secure, resilient, and future-ready.**

As Indian MSMEs rapidly adopt digital payments, cloud platforms, GST systems, e-commerce, and AI-driven tools, cybersecurity has emerged as one of the biggest business continuity challenges of the digital era. From phishing scams and payment fraud to ransomware attacks and data theft, cyber threats are increasingly targeting small businesses that often operate with limited digital safeguards. In this exclusive conversation with BizIgnite, Tarun Wig shares practical insights on the cyber risks facing MSMEs, the role of AI in modern cybersecurity, and the simple yet powerful steps businesses can take to protect themselves in a connected economy.

What exactly is cybersecurity, and why is it so important for MSMEs today?

Mr. Wig: Cybersecurity is the process of protecting systems, data, financial records, and digital operations from cyberattacks using technology, processes, and security practices. In simple terms, it is like locking your business premises every night—except the digital locks need to work across multiple layers.

Today, MSMEs use UPI payments, GST portals, cloud software, e-commerce platforms, and online banking daily. Every digital touchpoint creates a potential vulnerability. A single cyberattack can disrupt operations, freeze systems through ransomware, or even drain bank accounts. One of the biggest misconceptions among MSMEs is believing they are “too small” to be targeted. In reality, cybercriminals often target smaller businesses because they assume defenses are weaker. That makes cybersecurity a survival issue, not just a technology issue.

How vulnerable are MSMEs to cyber threats in India today?

Mr. Wig: The belief that only large companies face cyber threats is one of the most dangerous myths in business today. Attackers go where protection is weakest, and MSMEs are increasingly becoming preferred targets.

Some of the most common attacks include:

- Phishing emails pretending to be banks or vendors to steal login credentials
- Ransomware attacks that encrypt business data and demand payment
- Business Email Compromise (BEC) where attackers redirect payments into fake accounts
- Data breaches involving theft and sale of customer information

These are not isolated incidents. Businesses across Tier 2 and Tier 3 cities are already facing such attacks. In one case, a textile exporter reportedly lost more than ₹40 lakh due to a spoofed email. The financial and reputational damage from even a single incident can be devastating for a small business.

What lessons can MSMEs learn from national cybersecurity strategies?

Mr. Wig: India's cybersecurity philosophy is built on three principles: anticipate threats, minimise exposure, and respond quickly. MSMEs can adopt the same approach at their own scale.

The **first step** is identifying and protecting critical information such as customer records, payment credentials, and financial data. Businesses should apply stronger controls around their most sensitive assets.

Second, MSMEs should adopt an intelligence-led approach. National agencies do not wait for attacks to happen. Similarly, businesses can use AI-enabled tools to identify suspicious activity early and reduce risk proactively.

Third, resilience is as important as resistance. Businesses should maintain offline backups, create a basic incident response plan, and know whom to contact in case of an attack—whether it is the bank fraud desk, a cybersecurity consultant, or CERT-In. Preparedness significantly reduces damage during a crisis.

How can MSMEs move from reactive security to predictive, AI-driven cybersecurity?

Mr. Wig: The traditional mindset of "we will deal with it when it happens" is extremely expensive in the digital age. Recovery costs after a breach—including operational disruption, legal exposure, and customer loss—are often far higher than preventive investments.

The good news is that **predictive cybersecurity no longer requires massive IT budgets**. Many AI-powered cybersecurity solutions are now available through affordable SaaS subscription models, making them accessible even to smaller enterprises.

These systems continuously monitor email activity, network behaviour, and login patterns to detect anomalies before they escalate into major incidents.

A practical starting point for MSMEs is AI-powered email protection, which blocks most phishing and spoofing attacks. Businesses can then gradually add automated alerts for suspicious logins, endpoint protection, and network monitoring solutions.

The key is to start small and scale steadily instead of waiting for a perfect, enterprise-level system. Even businesses with 10–50 employees can now access affordable managed detection and response services.

What are some simple AI-powered cybersecurity tools MSMEs can start using immediately?

Mr. Wig: AI in cybersecurity does not mean hiring a data science team. It simply means using intelligent tools that can identify threats faster than manual systems.

For example:

- Microsoft Defender for Business and Google Workspace AI-based security can detect phishing emails and spoofed senders in real time. Many businesses already have access to these tools through existing subscriptions.

- AI-enabled banking systems can flag suspicious transactions, such as unusual transfers at odd hours, and pause them for verification.
- Endpoint Detection and Response (EDR) platforms use AI to monitor devices and automatically isolate threats before they spread across systems.

The objective is to quietly automate protection in the background so business owners can focus on operations and growth.

What are the first steps MSME leaders should take to build a cyber-secure organisation?

Mr. Wig: Cybersecurity must start at the leadership level. When business owners treat cybersecurity seriously, the entire organisation follows.

The first step is conducting a Digital Risk Audit. Businesses need to identify all digital tools they use and determine who has access to sensitive data.

Next comes basic digital hygiene:

- Enable multi-factor authentication across accounts
- Use a password manager
- Maintain regular backups

These simple measures alone can prevent a large percentage of common attacks. Employee awareness is equally important. Even a short quarterly session on phishing detection and payment verification can prevent major financial losses. Businesses should also establish a **basic Cyber Incident Response Plan** so employees know exactly what to do if an attack occurs.

Finally, MSMEs should consider periodic guidance from a cybersecurity expert or advisor. Even limited external support can help businesses strengthen their digital posture significantly.

Cybersecurity is not merely an IT concern—it is a business continuity priority that demands leadership attention, planning, and consistent execution.◆

The 5-Step Organizational Blueprint for Cyber Resilience

Digital Risk Audit	Identify every digital tool in use and audit who has access to sensitive data. You cannot defend that which you do not see.
Unbreakable Hygiene	Implement MultiFactor Authentication (MFA), use password managers, and maintain strict, regular backups.
Employee Calibration	Conduct a 30-minute quarterly training session on spotting phishing and verifying vendor payments.
Incident Response Plan	Establish a clear, documented protocol so the team knows exactly what steps to take the moment an attack occurs.
Expert Oversight	Engage a part-time cybersecurity advisor to review organizational posture on a quarterly basis.