TATA Tele Business Services | BOBig

TATA Tele Business Services SME Digital INSIGHTS Powered by CMR

From Reactive to Real-Time

The Strategic Imperative for SME Cybersecurity

SME Digital Insights on Cybersecurity Study

Tata Tele Business Services & CyberMedia Research (CMR)

FOREWORD

India's digital economy is expanding at an exceptional pace, transforming SMEs from digital consumers to critical components of enterprise supply chains. Cloud adoption is now table stakes. Digital platforms now drive revenue channels. Yet this rapid modernization has created a structural vulnerability: cybersecurity governance has not evolved at the same pace as digital infrastructure. The result is measurable risk exposure growing exponentially within an always-on threat environment dominated by relentless, high-velocity cyber threats, replacing the slower, stealth-driven attacks of the past.

The Tata Tele Business Services SME Digital Insights on Cybersecurity, conducted in association with CyberMedia Research (CMR), India's leading trusted technology research and advisory firm, is grounded in primary research spanning 800 IT decision-makers and business leaders across micro, small, and medium enterprises in major Indian cities.

The study insights point to a critical mismatch between awareness and execution.

While 84% of SME leaders plan to increase cybersecurity spending within the next 12 to 24 months, a majority of SMEs are progressing from periodic reviews toward more continuous security oversight practices, despite facing cyber threats capable of evolving and executing within minutes. Specifically, 35% of organizations conduct security reviews only on a quarterly or half-yearly basis, while another 26% rely on ad-hoc security practices.

The operational implications are concrete and quantifiable.

Threat actors do not operate on a quarterly calendar. Phishing campaigns execute in minutes. Credential compromise occurs in the hour following initial contact. Lateral movement across networks progresses over days.

In an organization operating on a quarterly review cycle, none of this activity registers until the next scheduled assessment—by which time data exfiltration is complete, customer trust is compromised, and regulatory exposure is established as fact rather than potential.

This white paper establishes the business case for a strategic shift in cybersecurity governance: from interval-based, reactive security reviews to continuous, real-time monitoring and threat detection. It assesses current SME maturity, identifies the barriers preventing transition, and outlines the process and technology requirements for organizations moving from detection-after-damage to containment-before-consequence schema.

The critical finding: this transition does not require building security operations centres in-house. It requires structured partnerships with trusted partners and managed security providers whose 24/7 monitoring, threat intelligence, and incident response expertise can be embedded into SME operations sustainably.

The bottom line: the transition from "detect-after-damage" to "contain-before-consequence" is imperative. For CXOs and IT leaders, this report provides the quantified business case, the risk analysis, and the actionable roadmap to get there.

Table of Contents

The Detection Gap: Securing a Continuous Business with Periodic Oversight

Indian SMEs have rapidly embraced digital transformation. Cloud adoption is now mainstream, while e-commerce and digital engagement channels have become central to customer acquisition, operations, and revenue generation. However, Cybersecurity governance is evolving alongside digital transformation, creating opportunities to further strengthen resilience. Many SMEs have established foundational security practices and are now progressing toward more continuous and proactive security models.

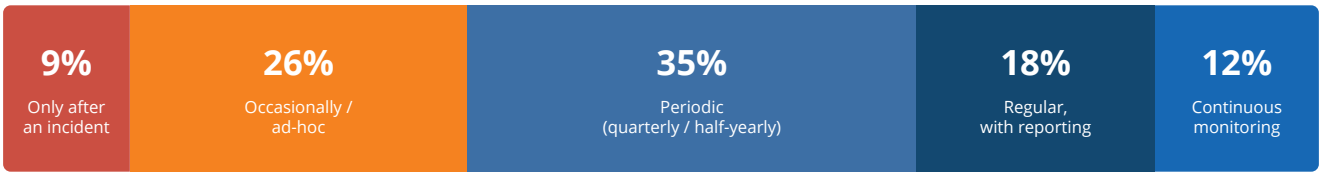
70%
SMEs have a reactive Cybersecurity posture

40%
SMEs experienced a cybersecurity incident in the last 24 months

The gap is stark. Our research shows that 35% of Indian SMEs conduct cybersecurity reviews only quarterly or half-yearly, making it the single largest operating model. Another 26% approach cybersecurity on an ad-hoc basis, responding only when an incident or visible disruption occurs. In total, more than six in ten SMEs continue to operate with extended periods of limited or no continuous security oversight.

The operational consequences are already becoming visible. Among SMEs that experienced cybersecurity incidents, 19% reported business disruption or operational downtime, while 17% experienced data leakage or loss and 15% reported unauthorized access to systems or information. These outcomes reinforce that delayed detection is no longer confined to technology functions; it increasingly translates into business disruption, operational risk, and weaker organizational resilience.

How Frequently Do SMEs Review Cybersecurity?



This creates a growing opportunity to align security operations with business needs. Cyber threats no longer unfold over months. Phishing campaigns, credential compromise, and unauthorized access can occur within hours. Once inside a network, attackers establish persistence, move laterally across systems, identify critical assets, and begin data exfiltration long before a periodic review cycle begins. In organizations dependent on quarterly assessments, these attacks often remain invisible until compromise, data loss, customer impact, or regulatory exposure has already occurred.

Despite this reality, only 12% of SMEs surveyed have implemented continuous 24/7 monitoring capabilities, while another 18% conduct regular reviews supported by structured reporting mechanisms. The majority remain dependent on interval-based security practices designed for a slower, pre-continuous-threat environment.

30%
SMEs have a proactive Cybersecurity posture

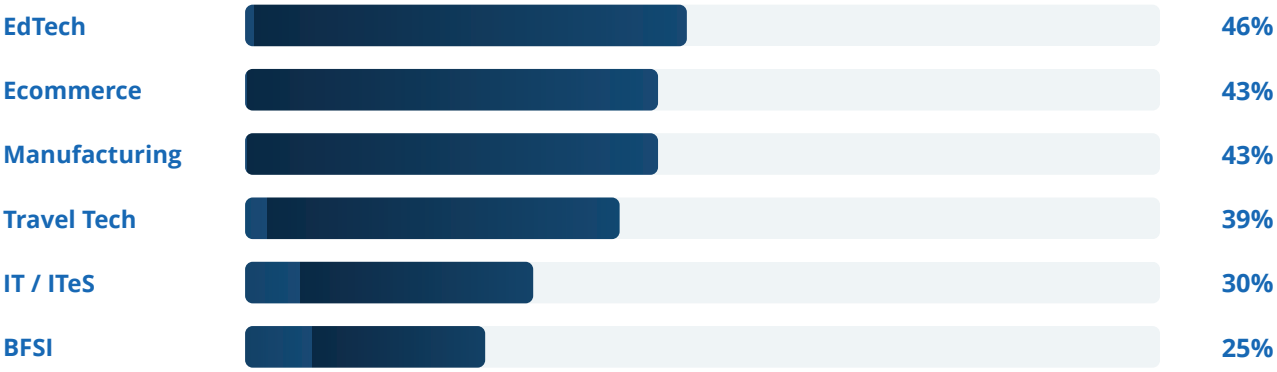
The asymmetry is structural. Indian SMEs are operating always-on digital businesses while relying on security oversight models built around periodic visibility. In modern cybersecurity, delayed detection is no longer an operational inefficiency. It is a direct business risk.

The Maturity Paradox: Digital-First Businesses, Evolving Security Operations

The research reveals a critical insight: digital infrastructure maturity has not translated into cybersecurity governance maturity. Across India's most digitally native and data-intensive sectors—IT/ITeS, eCommerce, and BFSI—periodic security reviews remain the predominant operating model, despite regulatory requirements, customer expectations, and operational risk that should mandate continuous oversight.

Within IT/ITeS companies, nearly 30% of surveyed organizations still rely on quarterly or half-yearly security reviews. In e-commerce, the figure rises to 43%, while in BFSI, despite stringent regulatory oversight, 25% of organizations continue to operate on the same periodic review cadence.

Cybersecurity Review Frequency by Industry
Even Digital-First Sectors Rely Heavily on Periodic Reviews



These findings challenge the assumption that digital maturity automatically translates to cybersecurity maturity. Organizations that have invested substantially in cloud infrastructure, digital commerce platforms, and data-intensive operations are simultaneously running security review cycles that cannot detect threats operating on a timeline of hours or days.

The mismatch between perceived cybersecurity readiness and operational maturity becomes even more apparent when organizations assess their own security posture against the quality of their monitoring capabilities. While a relatively small group has successfully aligned confidence with continuous monitoring, many SMEs either underestimate or overestimate their operational preparedness, reinforcing the need for greater visibility-led cybersecurity models.

The Confidence Gap Matrix Self-Rated Security Level vs. Monitoring Quality

The barrier is not awareness. SME leaders in these digitally mature sectors clearly understand the threat landscape and have lived through incidents that demonstrate the operational risk. The barrier is operational capacity, and specifically, the ability to deploy, manage, and sustain 24/7 security monitoring infrastructure without cannibalizing resources from core technology operations. In-house IT teams already managing cloud platforms, application stacks, and user support lack the dedicated focus and forensic expertise that continuous, real-time threat detection demands.

For digitally native, data-intensive organizations, the strategic opportunity lies not in further awareness-building, but in de-risking the operational execution of continuous monitoring through specialized, accountable partners. The question is not whether continuous monitoring is necessary; the market and regulators have settled that. The question is how to achieve it without the capital expense, talent cost, and operational friction of building in-house SOC infrastructure.

This is where managed security partnerships create a structural advantage.

> *"We are fairly confident, but we are not fully prepared for future threats."*
> **IT MANAGER, IT/ITES SMALL ENTERPRISE**

The Detection Gap: Why Timing Is the Defining Variable in Cybersecurity

Modern cyberattacks do not unfold over months. They unfold in hours.

A phishing email is delivered. An employee clicks the link. Credentials are compromised within the hour. The attacker gains access, begins reconnaissance, moves laterally across systems, identifies high-value assets, and starts preparing for data exfiltration.

In organizations with continuous monitoring, this activity is detected almost immediately. Alerts trigger in real time. Accounts are disabled. Access is contained before persistence is established or data is extracted. Incident duration is measured in minutes. Operational impact remains limited.

In organizations dependent on quarterly or periodic security reviews, the same attack often remains completely invisible. No alerts. No detection. Attackers operate undisturbed for weeks or months, mapping systems, escalating privileges, and extracting sensitive data long before the next scheduled assessment begins. By the time the breach is discovered, customer impact, operational disruption, regulatory exposure, and reputational damage are already established realities.

Two Outcomes, One Attack

Continuous Monitoring

1. Phishing email arrives
2. Employee clicks the link
3. Credentials compromised
4. Alert fires within minutes
5. Account locked, threat contained

Detected in minutes to 1 hour. Damage prevented.

Quarterly / Periodic Review

1. Phishing email arrives
2. Employee clicks the link
3. Credentials compromised
4. Attacker moves laterally, undetected

Detected in weeks to months. Damage multiplies.

In an organization operating on a quarterly review cycle: The initial compromise, lateral movement, and reconnaissance phase remain completely invisible. No alerts. No detection. The attacker has weeks or months to establish persistence, enumerate systems, identify data repositories, and execute exfiltration. The breach is finally discovered—if at all—through external indicators: customer complaints, transaction anomalies, or regulatory notification. Incident duration: weeks to months. Data loss: substantial. Regulatory exposure: established.

This is not a hypothetical scenario. SME leaders described these failures directly during the research.

> *"We only realized something was wrong when customers started calling us about issues they were facing. Internally, there were no alerts or indicators that flagged the problem earlier. By the time we reacted, the issue had already impacted multiple users."*
>
> **IT MANAGER, HEALTHCARE SMALL ENTERPRISE**

> *"The issue was identified when transaction records did not match expected values during reconciliation. There was no prior alert or system trigger indicating a problem."*
>
> **DIRECTOR, BFSI MEDIUM ENTERPRISE**

These incidents were not detected through monitoring systems. They surfaced through customer complaints, transaction inconsistencies, and operational disruption.

> *"We believe our systems are secure, but manual processes can still create errors."*
> **IT MANAGER, MANUFACTURING MICRO ENTERPRISE**

Following a security incident, SMEs most commonly strengthen their technology posture, while a growing proportion also turn to specialist partners and simplified security architectures to improve long-term resilience.

60%
Upgraded Security Tools
Strengthened defenses by upgrading or adding security tools and technologies

41%
Engaged Managed Security Provider
Partnered with a managed security provider for expert monitoring and response

33%
Simplified Security Environment
Consolidated and streamlined tools to reduce complexity and improve efficiency.

AI Is Shrinking the Cyber Decision Window for Indian SMEs

Artificial intelligence is accelerating both sides of the cybersecurity equation for Indian SMEs, acting as a powerful threat multiplier while rapidly emerging as a vital defensive capability.

65%
SMEs fear AI attacks they cannot visualise

Our research shows that 65% of SMEs consider AI-driven attacks a threat they cannot fully visualize or defend against. At the same time, 34% expect AI-driven cyber threats to materially impact their business over the next 12–24 months. Looking beyond AI, SMEs also identify data leakage (42%), cloud security risks (40%), financial fraud (36%) and identity-based attacks (33%) among their leading cybersecurity concerns.

SME leaders describe the changing threat landscape in stark operational terms. AI enables automated vulnerability scanning that identifies weaknesses faster than internal teams can remediate them.

AI-generated phishing campaigns have become highly convincing at scale, often indistinguishable from legitimate communications. Legacy signature-based tools are fundamentally ill-equipped to detect these new attack patterns, while many Indian organizations continue to align their data environments with global AI security standards and DPDPA compliance.

> *"If AI-driven attacks compromise patient systems or diagnostics, the impact is immediate. We cannot afford that kind of uncertainty."*
>
> **IT HEAD, HEALTHCARE SMALL ENTERPRISE**

For organizations relying on quarterly or ad-hoc security reviews, AI further compresses an already inadequate detection window. However, the same data reveals a significant opportunity: 35% of SMEs view AI as a cybersecurity enabler, with the potential to accelerate threat detection, automate routine monitoring, and deliver stronger, more accessible protection to organizations unable to maintain large in-house security teams.

35%
SMEs see AI as a cybersecurity enabler

AI is expected to strengthen cybersecurity capabilities for SMEs:

- Threat Detection Will Become Faster: AI is expected to help identify suspicious activities and emerging threats before they escalate into incidents.
- Security Operations Will Become More Automated: SMEs expect AI to reduce dependence on manual monitoring and streamline security workflows.
- Response Times Will Improve: AI is seen as a way to accelerate investigation, prioritization, and mitigation of cyber incidents.
- Cybersecurity Will Become More Accessible: AI is expected to bring enterprise-grade security capabilities within reach of resource-constrained SMEs.

> *"AI is changing the threat landscape, but it is also becoming one of the most effective tools to help us detect, respond to, and manage cyber risks faster."*
>
> **IT MANAGER, E-COMMERCE MICRO ENTERPRISE**

The very AI capabilities reshaping the threat landscape are simultaneously redefining what effective continuous monitoring looks like. SMEs stand to gain the greatest advantage when they work with partners who can operationalize AI-aware detection and response rather than simply adding another disconnected tool to an already fragmented security stack.

The Regional Divide: Four Maturity Curves, One Cybersecurity Imperative

While Indian SMEs share the common challenge of transitioning from periodic security reviews to continuous protection, the pace of this journey differs across regions. Variations in governance maturity, investment priorities, operational capabilities, and monitoring practices reveal that organizations are progressing along different cybersecurity maturity curves. Rather than indicating stronger or weaker markets, these differences highlight distinct regional priorities that technology partners and SME leaders must address to accelerate cyber resilience.

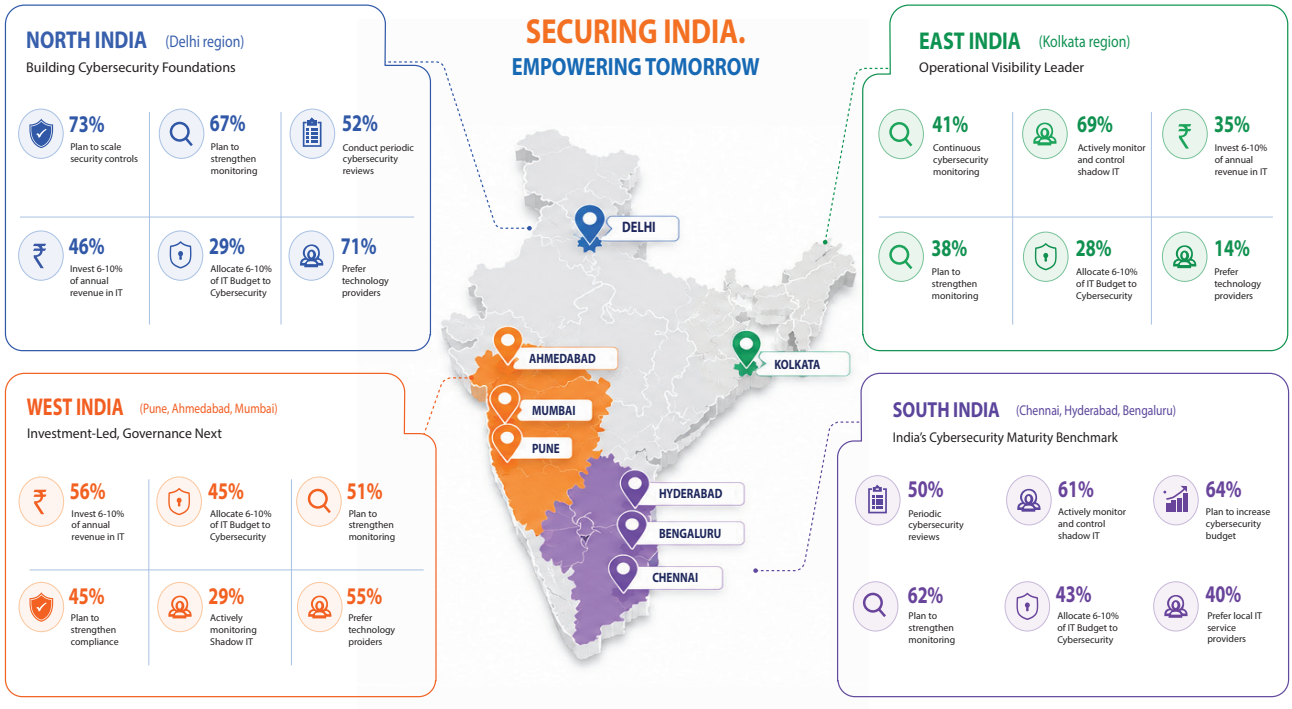
NORTH INDIA: SMEs are strengthening their cybersecurity foundations through strong future investment intent. SMEs plan to scale security controls, while two-thirds intend to strengthen monitoring capabilities over the next 12–24 months. Over half (52%) continue to rely on periodic cybersecurity reviews. The next step is converting this investment momentum into stronger governance, continuous monitoring, and day-to-day operational resilience.

73%
SMEs plan to scale security controls in next 12-24 months

EAST INDIA: SMEs are demonstrating strong operational cybersecurity maturity, with 69% actively monitoring Shadow IT and organizations placing greater emphasis on continuous monitoring. The region illustrates how sustained focus on operational visibility and structured security practices can strengthen cyber resilience. As digital adoption continues to grow, East India is well positioned to further advance its cybersecurity capabilities.

41%
SMEs review cybersecurity continuously

Cybersecurity Landscape by Region



*Map not to scale. This map is an original illustrative artwork prepared for this publication and is not intended to constitute an official or authoritative map. The depiction of India's boundaries is intended to be consistent with the territorial boundaries recognized by the Government of India.

WEST INDIA: Organizations across West India are advancing their cybersecurity journey through sustained technology investments and expanding operational capabilities, with 45% allocating 6–10% of their IT budget to cybersecurity. As businesses continue expanding their digital footprint, the focus is increasingly shifting toward strengthening governance, visibility, and continuous monitoring. This positions the region to translate technology investments into stronger long-term cybersecurity resilience.

56%
Allocate 6-10% of annual revenue to IT

SOUTH INDIA: South India continues to demonstrate a well-balanced approach to cybersecurity, combining strong governance practices with sustained investment. Organizations are strengthening monitoring, improving visibility, and reinforcing cybersecurity as an ongoing business discipline, while 61% of SMEs plan to increase their security budget over the coming year. The region highlights how operational maturity is built through the consistent alignment of technology, governance, and execution.

61%
SMEs actively monitor and control shadow IT

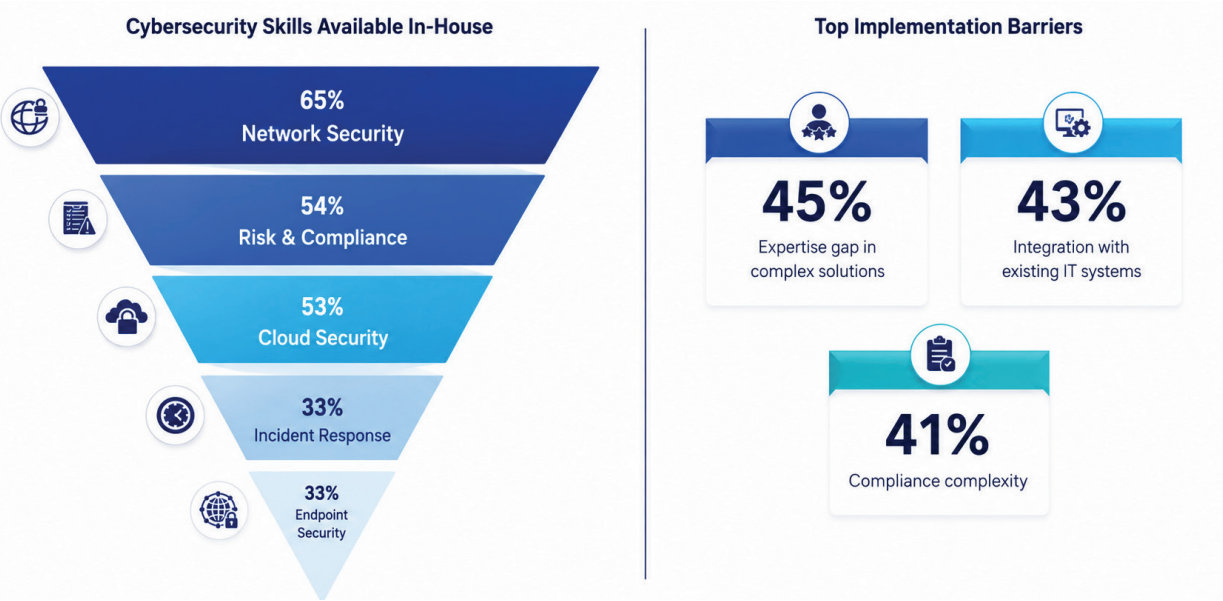
Across regions, cybersecurity maturity is increasingly defined not by technology investment alone, but by how effectively organizations operationalize security. While regional priorities differ, the direction is consistent. Indian SMEs are steadily moving beyond periodic, reactive security practices toward continuous, real-time cybersecurity operations that strengthen long-term business resilience.

Despite these regional differences, one pattern remains consistent across Indian SMEs. Cybersecurity strategies continue to evolve incrementally, with many organizations strengthening security in response to individual risks rather than through integrated, long-term cybersecurity planning. As digital environments become more complex, fragmented approaches are increasingly giving way to the need for coordinated, continuously managed security operations.

Building Cybersecurity Expertise at Scale: Why SMEs Need Specialist Support

The primary barrier to effective cybersecurity is no longer awareness. It is operational capability.

Our research identifies the expertise gap as the single largest obstacle to effective cybersecurity implementation, cited by 45% of SMEs, exceeding both integration complexity (43%) and budget constraints (23%).



While SMEs have established stronger capabilities in foundational areas, maturity varies significantly across more specialized cybersecurity functions.

Key strengths include:

• **Network Security:** Around 65% of SMEs report having in-house network security capabilities, making it one of the strongest cybersecurity competencies across organizations and providing a solid foundation for securing increasingly connected digital environments.

• **Risk & Compliance:** More than half (54%) of SMEs have developed internal risk and compliance capabilities, reflecting growing recognition of governance and regulatory readiness as integral components of cybersecurity resilience.

The capability gaps are significant:

• **Incident response:** Only 33% have this capability in-house. When something goes wrong, two-thirds of SMEs lack a defined incident response capability.

• **Cloud security expertise:** Just 53% report having internal cloud security expertise, despite cloud infrastructure now underpinning core business operations.

• **Endpoint security management:** Despite widespread deployment of endpoint security tools, only 33% of SMEs report confidence in managing them effectively, revealing a growing gap between tool adoption and operational proficiency.

Governance maturity also varies regionally, with Shadow IT visibility significantly stronger in some regions than others. SMEs in South India demonstrate relatively stronger Shadow IT visibility and governance practices, while other regions continue to strengthen monitoring and control mechanisms.

58%
SMEs have limited Shadow IT visibility

> *"While cybersecurity is acknowledged internally, it is not fully systematized or embedded into business processes. Decisions tend to happen in silos without a unified strategy. This makes execution inconsistent and dependent on individual teams."*
>
> **IT MANAGER, HEALTHCARE SMALL ENTERPRISE**

The operational reality is increasingly unsustainable. Internal IT teams are managing cloud infrastructure, applications, user support, and day-to-day operations simultaneously, while cybersecurity is treated as an additional responsibility layered onto existing workloads.

How Cyber Risk is Monitored

These operating models highlight that cybersecurity remains heavily dependent on manual intervention across many SMEs. As threat volumes continue to increase, manual oversight alone is becoming increasingly difficult to sustain at the speed and scale required for effective protection.

As a result, many SMEs continue to complement automated monitoring with manual oversight, creating opportunities to strengthen visibility, response speed, and operational efficiency through specialist support.

The challenge, therefore, is not simply deploying more security tools. It is building access to continuous monitoring, specialist expertise, and rapid response capabilities that most SMEs cannot realistically sustain in-house.

73%
SMEs are dissatisfied with the current setup

> *"Most of our monitoring is still manual, where teams periodically check systems instead of relying on automated alerts or centralized dashboards. Because of this, we end up depending on people to keep checking things, and sometimes things get missed."*
>
> **IT MANAGER, MANUFACTURING SMALL ENTERPRISE**

Despite these constraints, investment intent is demonstrably strong. 81% among micro enterprises, 84% among small enterprises, and 89% among medium enterprises. SMEs are prepared to commit resources.

The opportunity is to translate this strong investment intent into continuous monitoring, specialist expertise, and faster response capabilities.

84%
SMEs plan to increase cyber investment in next 12-24 months

Cybersecurity Investment Intent (Next 12-24 Month)

The opportunity is to translate this strong investment intent into continuous monitoring, specialist expertise, and faster response capabilities.

Cybersecurity investment intent is increasingly associated with operational maturity, not simply past incident exposure. The research shows that organizations with higher investment intent are more likely to have already established stronger foundations across monitoring, governance and cybersecurity budget allocation. Continuous monitoring emerges as the clearest differentiator: 53% of very-high-intent SMEs have continuous monitoring in place, compared with 15% among low/neutral-intent organizations.

Higher-intent organizations are also more likely to have a documented cybersecurity strategy with a defined budget (33%) and allocate more than 6% of their IT budget to cybersecurity (57%), indicating that future investment is increasingly linked to strengthening an existing security foundation rather than responding only to immediate gaps.

What differentiates SMEs with higher cybersecurity investment intent

	LOW / NEUTRAL	VERY HIGH	GAP
Continuous monitoring in place	15%	53%	+38 pp
Have a documented cybersecurity strategy with a defined budget	8%	33%	+25 pp
Allocate >6% of IT budget for Cybersecurity	32%	57%	+25 pp
Plan to strengthen monitoring over the next 12-24 months	42%	65%	+23 pp
Centrally governed with roadmap & ownership	2%	17%	+15 pp
Experienced >1 cyber incident in last 24 month	40%	37%	-3 pp

Extending the Security Team: The Role of Specialist Cybersecurity Expertise

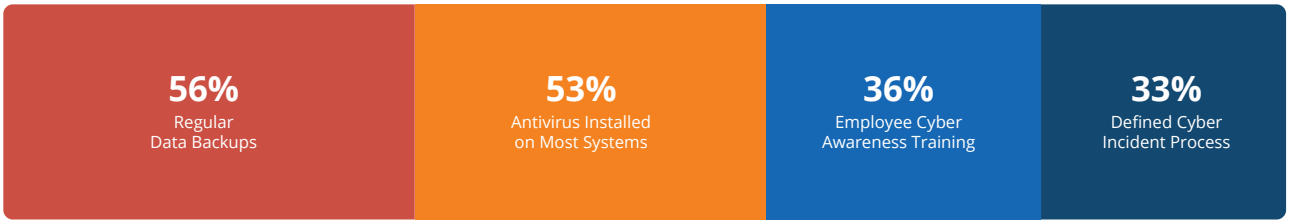
For most SMEs, building an in-house capability for continuous monitoring is neither practical nor economically viable.

As organizations evaluate specialist cybersecurity partners, operational considerations increasingly shape decision-making. Ease of integration (48%), quality of customer support (48%), trust and long-term relationships (46%), and security and compliance capabilities (45%) have emerged as the leading factors influencing partner selection. These priorities reinforce a broader shift toward service-led cybersecurity models designed to extend internal capabilities rather than simply add new technologies.

Sustaining 24/7 security operations requires specialized expertise, dedicated personnel, threat intelligence capabilities, and incident response readiness that few organizations can realistically develop and maintain at scale. Internal IT teams are already responsible for infrastructure, applications, cloud environments, user support, and business continuity. Adding round-the-clock security operations to that mandate creates operational strain and leaves critical gaps in visibility and response.

Most SMEs have already established the foundational elements of cybersecurity. Regular data backups and endpoint protection are now common practice, while employee awareness programmes and defined incident response processes are becoming increasingly prevalent.

Safeguards in Place Today



The more effective approach is to augment internal teams with specialist security expertise. Managed security partners provide capabilities that SMEs consistently struggle to build internally:

- **Continuous monitoring** — Real-time visibility and 24/7 oversight to identify and investigate threats as they emerge, rather than during periodic review cycles.
- **Expert-led detection and response** — Dedicated specialists who distinguish genuine threats from false positives and contain incidents before they escalate.
- **Accountability and ownership** — Defined service-level commitments, measurable response times, and clear responsibility for outcomes.

The objective is not to replace internal IT teams, but to extend their capabilities with the expertise, coverage, and operational discipline required to secure an always-on digital business environment. For SMEs, the path to stronger cybersecurity is not necessarily building more internal capacity, but gaining access to the specialized capabilities needed to operate at the speed of modern threats.

> *"We tend to rely on simpler tools that are easier to operate. There is always a trade-off between cost and capability."*
>
> IT MANAGER, E-COMMERCE MICRO ENTERPRISE

What SMEs Value Most from Security Partners

Beyond technical expertise, SMEs increasingly evaluate cybersecurity partners on their ability to simplify security operations and deliver measurable business outcomes. The findings indicate growing demand for integrated compliance support, simplified security management, and clearly defined service commitments that strengthen accountability while reducing operational complexity

> *"We are looking for partners who provide guidance and take ownership, not just tools. Clear outcomes and accountability matter more than features."*
>
> IT MANAGER, MANUFACTURING SMALL ENTERPRISE

The Trust Imperative: What SMEs Expect from Security Specialists

The research suggests that SMEs are seeking specialist support in areas where internal capability is difficult to build and sustain:

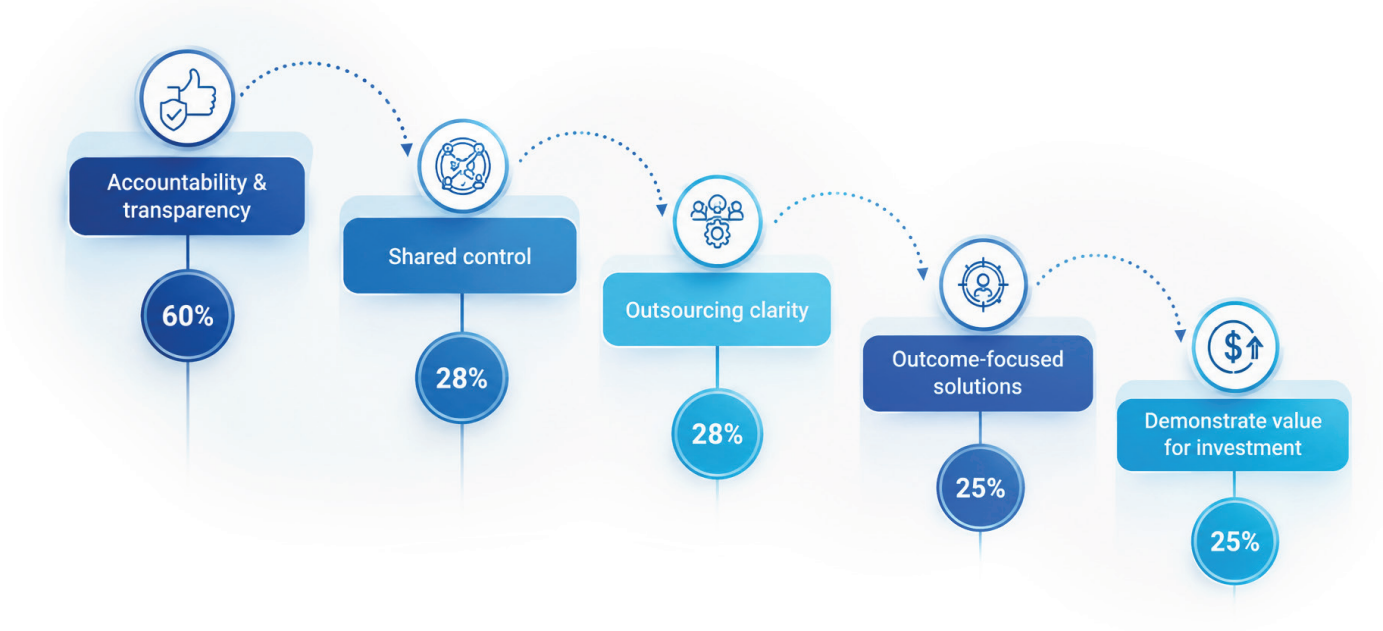
Specialized Expertise

Continuous monitoring, advanced threat detection, incident response, and security analytics demand specialized skills that many SMEs find difficult to develop and retain internally. Organizations expressed a clear preference for gaining access to experienced professionals without the need to establish a full-fledged security operations function from the ground up.

Accountability and Shared Ownership

SMEs emphasize the need for clearly defined roles and responsibilities, transparent escalation protocols, and assurance that security incidents will be handled promptly and effectively. This reflects a desire for partners who share ownership of outcomes rather than merely supplying tools or services.

What SMEs Need Most from a Trusted Security Partner



> *"Most solutions feel like product-driven offerings rather than solving our actual business problems. There is limited focus on outcomes or accountability."*
>
> **IT HEAD, IT/ITES MICRO ENTERPRISE**

Visibility and Control

Organizations want specialist support that enhances, not replaces, the oversight of their own environments. Real-time visibility into threats, incidents, and overall security posture remains essential for building confidence and trust. SMEs seek partners who provide clear, accessible dashboards and reporting mechanisms that allow them to stay informed about their security status at all times, enabling informed decision-making without surrendering control of their infrastructure or data.

Long-Term Partnership

SMEs increasingly value providers that act as an extension of their internal teams, bringing ongoing expertise, guidance, and operational support rather than simply deploying technology. This collaborative model helps bridge internal capability gaps while ensuring knowledge transfer over time. Visibility and transparency are therefore non-negotiable expectations, as they foster stronger alignment between the SME's business objectives and the partner's security practices.

> *"We are not always confident about how secure our data is when managed by external vendors. This lack of clarity makes outsourcing a risky decision."*
>
> **IT MANAGER, IT/ITES MICRO ENTERPRISE**

The message is clear: SMEs are looking to strengthen their internal security posture, not outsource accountability for it. The most successful cybersecurity models will therefore be those that combine internal business knowledge with external specialist expertise, creating a collaborative approach that improves security outcomes without compromising control.

Transparency in Pricing and SLAs

SMEs place high value on transparent pricing, clearly defined service-level agreements (SLAs), and predictable long-term engagement models. The research shows that clarity around costs, deliverables, and performance expectations is a key factor influencing their willingness to engage with security partners.

> *"Costs keep increasing with upgrades, and pricing is not always transparent, making it difficult to trust long-term value from vendors."*
>
> **IT MANAGER, IT/ITES MICRO ENTERPRISE**

When partners lead with accountability, transparency, and continuous engagement, trust follows. And when trust is there, SMEs are ready to invest.

The transition toward continuous cybersecurity is already underway. SMEs are increasingly prioritizing investments that strengthen operational visibility, governance, and resilience rather than simply expanding their security technology footprint.

Cybersecurity Priorities Over the Next 12–24 Months

The findings indicate that organizations are placing greater emphasis on improving monitoring capabilities, strengthening compliance readiness, and modernizing security controls to support long-term cyber resilience.

From Periodic Reviews to Continuous Protection: The Roadmap Forward

Our research reveals both the urgency and the opportunity for Indian SMEs to evolve their cybersecurity approach. The following strategic shifts are essential for organizations seeking to close the detection gap and build sustainable cyber resilience:

01 Adopt Always-On Security Monitoring

Modern cyber threats move at high velocity, while most Indian SMEs still rely on quarterly, half-yearly, or ad-hoc reviews. Organizations must shift to continuous 24/7 monitoring, real-time threat detection, and automated response to drastically shrink the window between compromise and containment.

02 Redirect Investments from Tools to Measurable Outcomes

Despite substantial technology investments, visibility and response effectiveness remain limited. Future cybersecurity spending should prioritize integrated capabilities that deliver tangible improvements in detection speed, incident containment, operational resilience, and overall risk reduction.

03 Bridge the Skills Gap with Specialist Operational Expertise

Expertise and operational capacity represent the biggest barrier to progress (cited by 45% of respondents). SMEs should prioritize access to specialized capabilities in continuous threat monitoring, incident response, cloud security, and security operations that are challenging to build and sustain internally.

04 Elevate Cybersecurity to a Core Business Resilience Priority

As digital infrastructure drives revenue, customer experience, and continuity, cybersecurity must evolve from a tactical IT function into a strategic enterprise risk and resilience imperative. Performance must be measured by business outcomes — Mean Time to Detect (MTTD), Mean Time to Contain (MTTC), reduced security-related downtime, and stakeholder trust.

05 Forge Trusted Security Partnerships to Scale Resilience

For the majority of Indian SMEs, maintaining enterprise-grade 24/7 monitoring, threat intelligence, and incident response in-house is impractical and cost-prohibitive. The most successful organizations will blend internal business insight with trusted managed security partners that deliver continuous protection, specialized expertise, real-time visibility, and full accountability for outcomes.

In Conclusion
The Future Belongs to Real-Time Security

The cybersecurity landscape for Indian SMEs has reached a structural inflection point. The periodic review model, built around quarterly assessments, manual monitoring, and reactive incident response, was designed for a threat environment that no longer exists. Today's cyber threats operate continuously, evolve rapidly, and exploit vulnerabilities long before traditional review cycles begin.

The findings from this study reveal a clear disconnect between intent and execution. While 84% of Indian SMEs plan to increase cybersecurity investment over the next 12 to 24 months, 61% continue to operate with intermittent security oversight. This disconnect points to a key operational challenge: translating planned investments into continuous visibility, faster detection, and timely response capabilities.

The challenge is no longer awareness, nor is it simply a question of budget. It is the ability to translate cybersecurity investment into continuous visibility, rapid detection, and timely response.

As Indian SMEs become increasingly digital, cybersecurity can no longer function effectively as a periodic compliance exercise. It must evolve into a real-time business capability, integrated into day-to-day operations with the same consistency as other critical functions, such as network availability and business continuity.

The data suggests that organizations making this transition toward continuous monitoring are better positioned to reduce incident impact, minimize operational disruption, strengthen regulatory compliance, and enhance stakeholder trust. The strategic priority for SME leaders is to accelerate this shift by combining internal resources with specialized expertise and trusted partnerships best suited to their scale and requirements.

About SME Digital Insights on Cybersecurity

The SME Digital Insights on Cybersecurity Study is a comprehensive analysis of cybersecurity readiness, implementation challenges, and emerging trends among Indian small and medium enterprises. The study explores how SMEs approach security today, where gaps exist, and what they need from partners to move from reactive to proactive protection. The research draws insights from 800 IT decision-makers and business leaders across micro, small, and medium enterprises in major Indian cities. The study covers diverse industry verticals, including IT/ITeS, eCommerce, Manufacturing, Banking and Financial Services, Healthcare Tech, EdTech, and Travel Tech.

For results based on a randomly chosen sample of this size, there is 95% confidence that the results have a statistical precision of plus or minus 5% of what they would be if the entire population had been surveyed.

Enterprise Classification

- **Micro Enterprises** — up to 50 employees
- **Small Enterprises** — 51 to 500 employees
- **Medium Enterprises** — 501 to 1,000+ employees

The research methodology combined quantitative and qualitative approaches to provide both statistical rigor and contextual depth, including:

- **Quantitative surveys** with IT decision-makers and senior business leaders
- **In-depth qualitative interviews** to capture real-world experiences and operational challenges

About Tata Tele Business Services

Tata Tele Business Services (TTBS), belonging to the prestigious Tata Group of Companies, is the country's leading enabler of connectivity and communication solutions for businesses. With services ranging from connectivity, collaboration, cloud, security, and marketing solutions, TTBS offers the largest portfolio of ICT services for businesses in India.

With an unwavering focus on customer centricity and innovation, TTBS continues to garner recognition from customers and peers alike. As businesses across India accelerate their digital transformation journeys, TTBS serves as a trusted partner, enabling SMEs to harness technology safely and effectively for sustainable growth.

TTBS's comprehensive cybersecurity offerings empower SMEs to:

- Move from periodic security reviews to continuous monitoring and protection
- Access expert-led managed security services without the overhead of building internal teams
- Gain real-time visibility into security posture through integrated dashboards
- Respond to threats in minutes, not months, with 24/7 monitoring and rapid incident response
- Navigate compliance requirements across industry regulations with specialist guidance
- Scale security capabilities seamlessly as business grows

Through deep industry expertise, proven methodologies, clear accountability, and commitment to customer success, TTBS enables Indian SMEs to operate with confidence in an increasingly connected world. TTBS does not just provide tools—it takes ownership of outcomes, delivers transparency, and builds long-term partnerships that transform cybersecurity from a concern into a competitive advantage.

For More Information

Email : dobig@tatatel.co.in , Website : www.tatatelebusiness.com

About CyberMedia Research (CMR)

CyberMedia Research (CMR) is part of CyberMedia, South Asia's foremost specialty media house, which has tracked the evolution of India's technology landscape for over four decades.

CMR itself carries over 15 years of research heritage, built on two decades of legacy research history before that — giving CMR one of the longest continuous track records in Indian technology research and advisory. Today, CMR delivers market intelligence, strategic consulting, and go-to-market support to large enterprises, small and medium enterprises, industry associations, and government organizations, helping them make confident decisions in fast-moving, rapidly evolving technology markets.

CMR's Industry Research Group brings deep, cross-sector expertise spanning consumer technology, enterprise IT, telecom, semiconductors, automotive, and cybersecurity — with primary research as its defining strength, backed by go-to-market capabilities.

This SME Digital Insights on Cybersecurity study, conducted in partnership with Tata Tele Business Services, reflects that approach: grounded in structured surveys and qualitative interviews with 800 IT decision-makers and business leaders across India, and designed to surface not just what SMEs are doing, but why — and where the gaps lie between intent and execution.

For More Information

Email: info@cmrindia.com • Website: www.cmrindia.com