November' 25 Edition

SOFFIT INFRASTRUCTURE SERVICES (P) LTD

soffit®
People • Process • Technology

The Tech Chronicle

Tech News that Powers Your World

Welcoming You to The Tech Chronicle!

This newsletter aims to keep you informed and engaged with the latest developments and insights from Soffit as well as from the industry. Our experts provide valuable guidance, ensuring that you can benefit from their knowledge and experience. We also bring you the latest industry news that keep u updated with emerging trends and developments that can impact your business.

Top Stories

Anoop PS
VP Managed Services
Technology & Projects

Featured Article

Cybersecurity Awareness Month 2025

"Stay Safe Online" & Our Shared Responsibility

Every October marks Cybersecurity Awareness Month, wakeup call for online safety and empowering individuals and organizations to better defend themselves from digital threats. In 2025, the campaign underscores the theme "Stay Safe Online," inviting everyone—from individuals and small businesses to critical infrastructure operators—to adopt simple yet powerful practices that make a difference.

While the landscape of cyber threats continues to evolve—accelerated by trends like AI-powered attacks, supply-chain vulnerabilities, and targeting of essential infrastructure—this awareness month reaffirms that security often starts with the individual and best practices.

The campaign encourages universal adoption of the core principles:

- Use strong, unique passwords and password managers
- Enable multi-factor authentication (MFA)
- Recognize and report phishing and suspicious behavior
- Update software regularly

These steps may seem simple, but they remain among the most effective defenses against cyberattacks. Indeed, human error and phishing still play outsized roles in successful breaches, especially when attackers exploit weak credentials or unpatched systems.

Why 2025 Matters: Identity, Infrastructure & the Rising Stakes

One emerging focus for 2025 and beyond is the prioritization of identity security, especially as many cyberattacks increasingly target access credentials and identity systems. With MFA adoption still uneven across organizations, protecting identity becomes a frontline defense. The emphasis is especially urgent for critical infrastructure sectors and smaller organizations that support essential services but often have fewer resources for cybersecurity resilience.

Meanwhile, attackers are increasingly exploiting artificial intelligence, supply chain gaps, and zero-day vulnerabilities, placing additional pressure on defenders to stay vigilant. Protecting the backbone of national systems - like energy grids, transport, utilities—requires not only technology investment, but also information sharing, real-time detection, and cross-sector coordination. As we observe Cybersecurity Awareness Month 2025, the message is clear: while technology must evolve, the human factor remains central.

Each person's action—or inaction—carries risk. By adopting simple security habits, engaging thoughtfully with emerging threats, and treating cybersecurity as a shared responsibility, we can collectively raise the baseline of defense.
Let's make October—and every day—one step closer to a safer, more resilient digital world.

IT Maturity Analysis Becomes a Key to Smarter Business Strategy

Soffit's newly launched IT Maturity Awareness initiative is emerging as a strategic enabler for forward-thinking businesses. By providing a clear, data-driven evaluation of existing IT capabilities and security gaps, Soffit empowers organizations to build actionable roadmaps that elevate IT maturity and strengthen cyber resilience. Through this initiative, businesses are not just closing operational gaps—they're transforming IT into a driver of growth and competitive advantage.

"Our clients don't just need technology, they need clarity. They want to understand exactly where they stand, identify the risks they face, and have a clear, actionable path to advance. Our IT maturity analysis delivers actionable insights that transforms IT from chaos to enabler. We're proud to empower businesses to build resilient IT that drives growth and protect their business operations,"

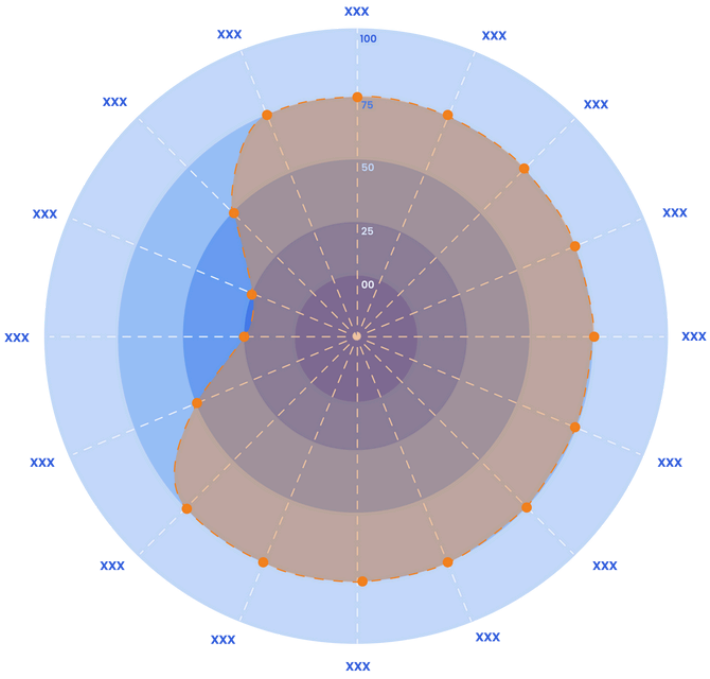
Saji Prabhakaran
Managing Director

Five Levels of IT Maturity: A Structured Pathway

The tool benchmarks organizations across five defined levels of IT maturity, enabling leaders to identify strengths, uncover risks, and align IT investments with business objectives:

- Reactive IT – Struggling with ad hoc fixes and firefighting, lacking long-term planning.
- Developing IT – Beginning to put structure in place but still facing gaps in governance and integration.
- Essential IT – Standardized practices, weaker controls, and growing focus on scalability..
- Advanced IT – Streamlined, data-driven, and proactive, with strong risk management.
- Transformative IT – A true business enabler, driving innovation, agility, and competitive growth

Each level provides a clear picture of where an organization stands today and what steps are required to advance toward greater resilience, security, and competitiveness.



Tailored Roadmaps for Every Business

Beyond just measurement, Soffit provides customized maturity roadmaps, helping businesses transition from reactive practices to transformative IT management. These roadmaps address core dimensions such as:

- Operations – streamlining processes for efficiency.
- Security – embedding cyber resilience.
- Governance – ensuring compliance and accountability.
- Innovation – leveraging AI, automation, and data-driven systems.

With cyber risks escalating and businesses relying more than ever on digital infrastructure, knowing one's IT maturity level is no longer optional—it's a strategic necessity. The IT Maturity Analysis Tool offers leaders an unbiased, comprehensive view of their IT landscape, enabling them to prioritize investments, reduce risks, and accelerate digital transformation.

CXO Viewpoint

AI and ML are Reshaping the Cybersecurity Landscape

Umashankar Lakshmipathy, EVP and Co-head of CIS and CyberSecurity, Infosys

Traditional threat detection methods, such as signature-based pattern matching, have been effective for identifying known threats. However, they fall short in detecting new or zero-day threats, including those augmented by AI. With its ability to analyze large volumes of data swiftly, infer patterns, and generate predictive insights, AI and ML enable real-time threat detection, significantly reducing the window of opportunity for attackers to exploit new vulnerabilities. Furthermore, AI and ML enhance threat intelligence by rapidly analyzing and correlating data from diverse sources to identify emerging threat patterns and contextualize risks – allowing proactive hunting of threats across the enterprise landscape. Read More >>>

When Workplace Politics Becomes a Cyber Threat

From a C-suite perspective, internal workplace politics can become a cybersecurity risk. When teams become fractured by ideological alignment, dissenting perspectives may be silenced or entirely excluded, leading to groupthink and blind spots in security strategy. That's particularly dangerous in cybersecurity, where weaknesses often lie in the margins: unchallenged assumptions, overlooked alerts, or suppressed warning signals from lower levels. By fostering an environment that deliberately de-escalates political friction, encourages diverse thinking, and enforces evidence-based governance, leadership can shield the organization from this hidden vulnerability. Read More >>>

Rethinking Vendor Risk Amid Geopolitical Tensions

Luke Ellery, VP Analyst, Gartner

Geopolitical tensions are reshaping vendor risk management, pushing CIOs to integrate geopolitical risk into assessments, contracts, and monitoring to ensure business continuity.

He emphasizes that geopolitical risks are now central to vendor risk management. He advises CIOs to proactively integrate these risks into vendor assessments, contract negotiations, and continuous monitoring to ensure business continuity in an increasingly volatile global environment. Read the full insights on >>>

Industry News

Why SEBI's Focus on Trading Glitches Highlights a Larger Cyber-Operational Risk

SEBI's latest proposal to refine rules around "technical glitches" in online trading platforms is a timely reminder of the growing intersection between cybersecurity and operational resilience in India's capital markets. As trading increasingly depends on automated and cloud-integrated platforms, even minor disruptions can cascade into large-scale financial and reputational risks.

For financial firms, this evolution calls for integrated IT and cybersecurity oversight, where proactive monitoring, redundancy planning, and incident response are not siloed functions but part of a unified resilience strategy. **Read the news on >>>**

Service Desks Becoming Prime Attack Vectors

Service desks are increasingly being targeted as entry points by threat actors. Attackers are leveraging social engineering techniques—often initiating what looks like a routine support call—to trick help desk agents into providing access or resetting credentials. For organizations, the lesson is clear: protect the service desk as a first line of defence, not a soft target. To defend against this threat, security teams are pushing for formalized, workflow-based verification processes rather than leaving judgment calls to agents.

Read the news on >>>

Cloud Isn't a Safety Net

Cloud providers typically guarantee the reliability of infrastructure: hardware uptime, network availability, and protection from data center failures. But they explicitly do not promise to safeguard against data corruption, user errors, application-level failures, or malicious deletion. As the article highlights, data backup and recovery remain a shared responsibility—the cloud provider protects the platform, but the customer must protect their data. This distinction is critical for any resilience strategy.

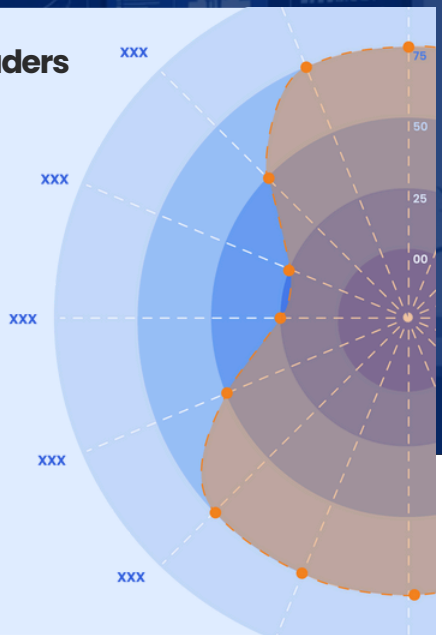
Read the news on >>

Soffit News

Soffit Rolls Out IT Maturity Analysis Initiative for Business Leaders

Soffit recently launched IT maturity analysis initiative, a new platform designed to raise awareness of each business's IT maturity level. Through this strategic effort, Soffit help businesses assess, benchmark, and accelerate their digital transformation journey. This evaluates organizational performance across 16 key IT domains, providing a clear, data-driven view of how effectively technology supports business growth, governance, and risk management.

Targeted at business heads, CXOs, compliance, and risk leaders, the platform enables businesses to identify strengths, uncover hidden gaps, and align IT strategies with evolving business priorities.
By delivering actionable insights, Soffit empowers organizations to make informed decisions that drive resilience, innovation, and long-term value. Businesses can now assess their IT maturity and schedule a personalized consultation at www.soffit.in/book-consultation.



Successful Firewall Migration for Long Standing NBFC Client

We're delighted to announce the successful completion of a firewall migration project for one of our long-standing clients in the Non-Banking Financial Company (NBFC) sector. This engagement focused on strengthening their network perimeter security while ensuring business continuity and regulatory compliance.

The project began with a comprehensive assessment of the existing firewall environment, including traffic analysis, policy review, and configuration mapping. Our team developed a meticulously planned migration roadmap, prioritizing zero downtime and uninterrupted protection for critical systems.

Javed Jose
Engineer IT Infra

Agil PS
Engineer IT Infra

Muhammed Labeeb
Engineer IT Infra

Vineesh VV
Sr. Engineer IT Infra

Ashigoskar Vishnu
Associate Engineer IT Infra

We implemented the new-generation firewall solution, ensuring seamless policy transfer, redundancy setup, and high availability configuration. Rigorous pre- and post-migration testing validated every component—from VPN tunnels and NAT rules to intrusion prevention and threat intelligence integrations.

Throughout the process, our engineers maintained transparent coordination with the client's IT and compliance teams, ensuring every transition aligned with their operational, audit, and security requirements. The migration was executed smoothly and on schedule, with no disruption to business operations.

The client commended Soffit's attention to detail, precision-driven execution, and commitment to operational continuity, recognizing our team's dedication to delivering secure, reliable, and scalable IT infrastructure.

With this upgraded firewall environment, the client now benefits from enhanced network visibility, faster threat detection, and improved security posture—all essential for safeguarding financial data and maintaining uninterrupted service delivery in today's evolving threat landscape.
This initiative involved transitioning critical security infrastructure with minimal downtime while maintaining uninterrupted protection for essential systems.

Stay connected

We hope you find this newsletter informative and valuable as you navigate the dynamic IT landscape. We value your feedback. Kindly feel free to send suggestions, comments, or any questions regarding our services/newsletter at newsletter@soffit.in

Thank you for your continued trust and partnership. Let's continue to work together!

Disclaimer

This newsletter provides valuable updates on industry trends, insights, and our latest offerings. We respect your privacy and are committed to safeguarding your information. If you no longer wish to receive these communications, you can unsubscribe at any time by responding ***"Unsubscribe"*** *to* ***newsletter@soffit.in***

soffit®
People • Process • Technology

Healthy IT,
Healty Business

IS 649645

www.soffit.in