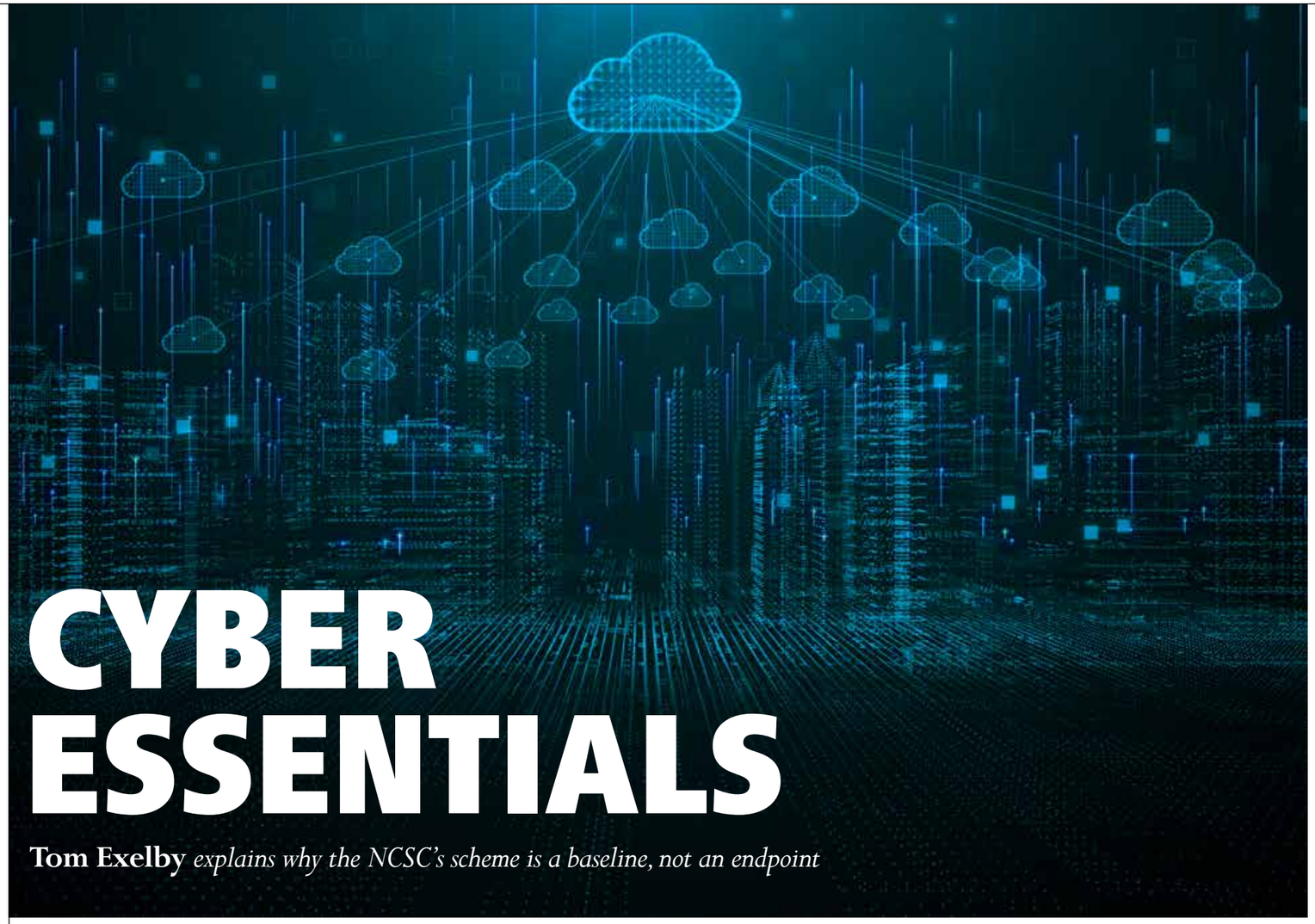

CYBER ESSENTIALS

Tom Exelby *explains why the NCSC's scheme is a baseline, not an endpoint*

For more than a decade, the National Cyber Security Centre's Cyber Essentials scheme has provided British organisations with a practical foundation for cyber security governance. It established a common baseline for security controls, improved access to public sector supply chains and helped thousands of SMEs address long-standing weaknesses in patching, administrative access, unsupported systems and endpoint protection.

That contribution still carries real value. Cyber Essentials remains one of the most accessible frameworks for improving cyber hygiene across smaller organisations, particularly those with limited internal security capability. Yet the threat landscape that shaped the scheme in 2014 no longer reflects the operational realities facing SMEs in 2026.

The attack surface facing organisations in 2026 is also considerably broader and more decentralised than it was when Cyber Essentials was introduced. In 2014, most SMEs operated within relatively contained corporate environments built around on-premise infrastructure, managed endpoints, and clearly defined network boundaries.

That model has since been replaced by highly distributed operating environments shaped by cloud adoption, remote working, SaaS dependency, connected IoT devices and widespread use of personal and unmanaged technology.

At the same time, the rapid adoption of generative AI tools has introduced a growing shadow AI problem, where employees use unapproved AI platforms outside formal governance controls, often exposing sensitive business data without visibility from security teams.

Many organisations now face a situation where identities, third-party integrations, APIs, smart devices and AI-enabled workflows create a far larger and less visible attack surface than traditional infrastructure alone.

The challenge for SMEs is no longer limited to securing servers and laptops. It increasingly involves understanding how unmanaged technologies, interconnected platforms and uncontrolled data flows alter operational risk across the business.

SMEs are increasingly being targeted because attackers now view them as commercially viable entry points into larger and more interconnected ecosystems. The CrowdStrike 2026 Global Threat Report highlights how modern intrusions increasingly rely on trusted identities, SaaS platforms, cloud services and supply chain relationships rather than traditional malware-based compromise.

In 2025, 82 percent of detections observed by CrowdStrike were malware-free, with attackers using valid credentials and authorised access pathways to blend into normal business activity. For many SMEs, this creates a difficult operating environment.

Smaller organisations often have less mature identity governance, fewer internal monitoring capabilities and limited visibility across cloud platforms and third-party integrations, making them attractive targets for credential theft, session hijacking and ransomware operations.

Smaller organisations often have less mature identity governance, fewer internal monitoring capabilities and limited visibility across cloud platforms

Attackers also recognise the strategic value of SMEs within supply chains. Compromising a smaller supplier, MSP or outsourced service provider can provide indirect access into larger enterprises and critical services without confronting heavily defended corporate environments directly.

At the same time, AI-enabled attack tooling is lowering the barrier to entry for cyber criminal groups, accelerating phishing campaigns, automating reconnaissance and reducing the time between initial compromise and lateral movement. CrowdStrike reported that the average breakout time fell to just 29 minutes in 2025, demonstrating how quickly attackers can exploit weaknesses once access is obtained.

Against this backdrop, Cyber Essentials should be viewed as a starting point rather than a complete security strategy. Baseline controls still reduce exposure to common threats, but certification alone does not address the identity, supply chain and operational resilience risks now shaping the modern threat landscape.

As regulation evolves through initiatives such as the proposed UK Cyber Security and Resilience Bill, the direction of travel is becoming clear. Organisations will increasingly be judged not simply on annual compliance exercises, but on their ability to maintain continuous cyber resilience across interconnected digital operations.

The industry still tends to discuss cyber attacks using outdated language centred on malware and exploits. In practice, modern intrusions increasingly begin with valid credentials. There are several reasons for this. First, cloud adoption has radically altered enterprise architecture. Applications now sit outside traditional network boundaries, accessed through browsers and identity platforms rather than internal VPNs.

Second, attackers have industrialised phishing operations. AI-generated lures, adversary-in-the-middle toolkits, phishing-as-a-service platforms, and token theft frameworks have lowered the barrier to entry dramatically. Third, identity attacks generate less operational noise than malware deployment. A successful login using legitimate credentials can evade traditional security tooling entirely. In a traditional breach scenario, an attacker exploited an unpatched vulnerability to gain code execution on a system. In a modern identity attack, the attacker simply authenticates as the user. That distinction changes defensive priorities. Even MFA, long viewed as a silver bullet, is now under sustained pressure from session hijacking, MFA fatigue attacks, reverse proxy phishing kits, and token replay techniques.

Recent reporting around long-running phishing campaigns targeting legacy authentication systems demonstrates how identity infrastructure itself has become a strategic target. At the same time, attackers are increasingly bypassing corporate controls through unmanaged devices and personal mobile workflows. QR code phishing campaigns surged sharply during early 2026 specifically, because they shifted user interaction away from monitored corporate endpoints.

CYBER ESSENTIALS IS ONE OF THE UK'S MOST COMMERCIALLY VALUABLE FRAMEWORKS

Identity telemetry, authentication monitoring, behavioural analytics and conditional access governance are no longer advanced security capabilities reserved for large enterprises. They are rapidly becoming baseline requirements.

Cyber Essentials still provides value because the fundamentals remain valid. Poor patching, weak configuration management and unrestricted administrative access continue to create avoidable exposure. But the baseline itself now requires expansion. A modern baseline should extend beyond the original five pillars into four additional operational disciplines.

Most organisations maintain detailed inventories of devices while possessing remarkably limited visibility over identities. Security leaders often know how many laptops exist, but cannot confidently answer: Which accounts possess privileged access? Which supplier identities retain persistent access? Which dormant accounts still authenticate? Which service accounts lack MFA? Which cloud applications possess excessive permissions?

Identity visibility is now as commercially significant as asset visibility. Without it, organisations cannot distinguish legitimate activity from compromised behaviour. This is particularly acute within cloud-native environments where users, APIs, AI agents, SaaS integrations and automation tools continuously exchange credentials and tokens outside traditional infrastructure controls. The future baseline must therefore focus on who is operating within the environment, not simply what device is connected.

Annual audits were sufficient when infrastructure changed slowly, but now they are increasingly disconnected from operational reality. Modern environments evolve constantly through SaaS onboarding, cloud deployments, remote access changes, supplier integrations and AI tooling adoption and static certification snapshots cannot keep pace with dynamic risk exposure.

Picture credit: AdobeStock

Continuous monitoring changes the operating model from retrospective assurance to real-time oversight. This is not about replacing Cyber Essentials audits, it is about recognising that annual validation alone no longer reflects how modern environments operate.

ANNUAL AUDITS ARE INCREASINGLY DISCONNECTED FROM OPERATIONAL REALITY

One of the more significant Cyber Essentials updates for this year is the removal of ambiguity around cloud scope. That matters because many organisations still apply traditional controls unevenly across hybrid environments. This challenge is widening further through AI adoption. Large language models, AI assistants, copilots and autonomous agents increasingly interact with sensitive corporate data using delegated permissions that is tied directly to identity systems.

Poorly governed AI deployments introduce a new category of operational exposure with things like excessive permissions, untracked data access, shadow AI usage, token leakage, third-party model integrations and automated decision workflows without oversight. Palo Alto Networks' 2026 incident response findings showed that 90 percent of incidents involved weak identity controls, while overprovisioned cloud permissions were nearly universal across analysed environments.

The central question is no longer whether organisations can stop every intrusion. It is whether they can continue operating during and after compromise. That distinction reshapes board-level priorities. Incident response plans can no longer exist solely as policy documents designed for audit purposes. They require operational rehearsal, executive participation, supplier coordination and measurable recovery objectives.

Cyber Essentials remains one of the UK's most commercially valuable cyber frameworks because it established a common starting point for organisations that previously lacked any structured security governance. That contribution should not be understated. But the operational environment surrounding the framework has fundamentally changed.

Identity compromise, cloud interconnectivity, AI-driven attacks and supply chain dependency have altered the economics of cyber intrusion. The next phase of cyber maturity will therefore depend less on annual certification and more on continuous visibility into users, privileges, authentication flows, supplier relationships and recovery readiness. The organisations that adapt fastest will not necessarily be those with the largest security budgets. They will be the ones that recognise a critical strategic truth: Cyber security is no longer primarily about protecting infrastructure. It is about maintaining trust in identity, continuity and operational resilience across an increasingly interconnected economy ●

Tom Exelby is Head of Cyber Security at Red Helix

Organisations will be judged on their ability to maintain continuous cyber resilience across interconnected digital operations

Picture credit: NCSC