UK Cyber Risk Landscape 2026: An External Audit Across Five Sectors

Foreword: From Oversight to Action

A Fresh Set of Eyes on the UK Cyber Risk Landscape

I've spent over 30 years working across IT infrastructure, risk management and regulated financial services — most recently as MD of my own business operating under FCA oversight. About two years ago I made a deliberate move toward a dedicated cyber role. I'm not going to pretend I arrived as an expert — I didn't. But I did arrive with two things I've never been able to shake: a risk management instinct honed in one of the most regulated industries in the UK, and a habit of building tools when I want to understand something and solve the problem properly.

So that's what I did...

Using a passive OSINT approach — nothing intrusive, no systems touched — I developed a scanning framework called Cyber-Vitals and ran it across 2,011 domains with a UK bias, spanning five sectors: Finance, Charities, Education, Manufacturing and SMEs. The goal was straightforward: what does the UK's external digital perimeter actually look like to an outside observer?

What I found surprised me — not because the vulnerabilities were exotic, but because of how consistently they appeared across sectors that should, on paper, know better.

I'm sharing this for two reasons. First because the data raises questions worth discussing openly. Second — and I'll be straight about this — I'm genuinely curious whether this confirms something the community is already seeing, or whether the patterns I've found at this scale add something new to the conversation.

Either way I'd rather ask the question than assume I already know the answer.

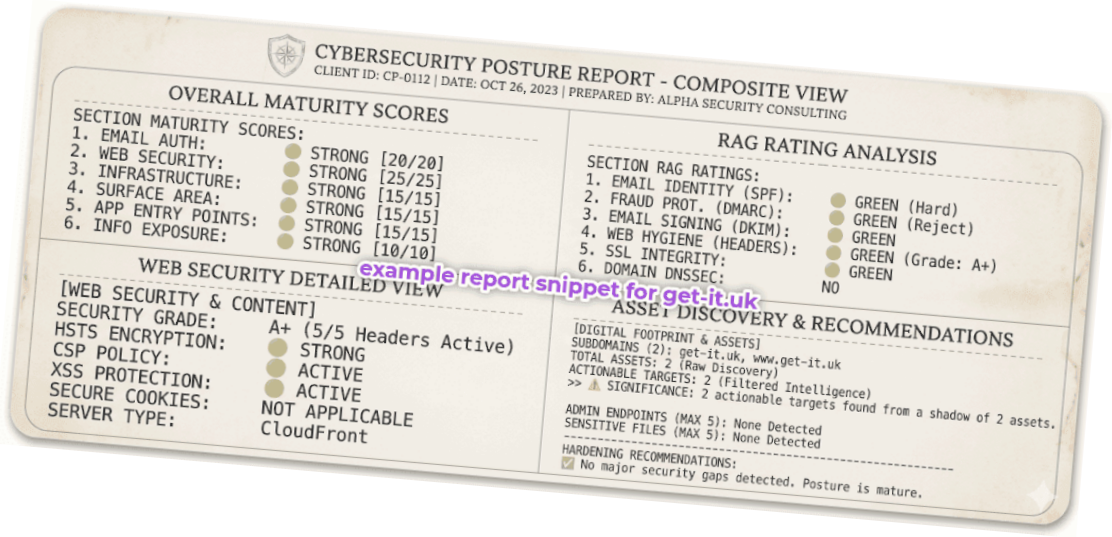
Franco Pietrantonio - *Lead Cyber Consultant, Get-It*

Methodology: The Cyber-Vitals Framework

An organisation cannot protect assets it does not know exist.

The 2026 Audit leverages the Cyber-Vitals engine to audit **N=2,011** unique domains across five cohorts (Tranco Global SME, UK Mid-Tier, UK FCA authorised Brokers, UK Charities, and Regional SMEs). The tool evaluates four key risk vectors:

1. **Identity Sovereignty (DNS/Email):** Analysing misconfigurations in SPF, DKIM, and DMARC that lead to "impersonation-ready" domains.
2. **Web Hygiene & Infrastructure:** Utilising the securityheaders.com grading system to identify vulnerabilities in the tech stack that are visible to any malicious actor.
3. **Discovery of Administrative Pathways:** Locating exposed setup files and admin panels that as best practice, should be obscured from public discovery.
4. **Legacy Asset Persistence:** Identifying "forgotten" files and previous version remnants. Our risk exposure score is partly based upon our finding here— It would take a much deeper dive to fully assess the true risk of these finding so we work on the basis, **an organisation cannot protect it's asset if it does not know they exist.**



As I only used passive testing, this analysis focuses exclusively on externally observable signals and does not assess internal controls, configurations, or compensating security measures

Key Market Findings

For reference, sector codes throughout this report are: FIN (Finance), CHA (Charity), EDU (Education), MAN (Manufacturing), GEN (General SME).

The "Half-Done" Phenomenon

A common trend we saw again and again in our scans were the organisations who appeared to have put the effort in for either their backend **or** the front end but so rarely both.This pattern may indicate a disconnect between front-end security controls and backend exposure management.

The data identifies a critical divergence where **60.5%** of firms maintain "polished" front-facing security but leave administrative pathways exposed. In the mid-range global cohort, **38.4%** broadcast an **Exposed Admin Portal**, while **32.4%** leaked **Sensitive Files**, including configuration backups.

> **In many cases, organisations are broadcasting more about their environment than they likely intend—information that could be leveraged by threat actors**

The Identity Vacuum

Within this dataset, 87.8% of domains lacked DMARC ‘reject’ enforcement, which may leave them vulnerable to brand impersonation. In high-stakes sectors like Insurance Brokerage and Financial Services, this represents a significant gap between regulatory intent and technical execution.

In the insurance sector for example, this gap could potentially be exploited to sabotage insurance coverage or a bad actor could use it for legitimate looking payment requests from the accounts department say.

In the charity sector, a donation drive appearing to come from a genuine email could be linking donors to a fake donation portal. For other organisations, variants or fake login portals could just as easily be utilised.

At scale, fragmented asset oversight may increase the risk of trust being exploited—where compromised or unmanaged assets can be leveraged to distribute credible-looking misinformation.

Large fragmented assets collections were observed multiple times within the dataset.

Sector Resilience Scorecard: 2026 Snapshot

Sector	Key audit Finding	Potential Risk Factor
FIN (Finance)	**The 'Decoy' Effect:** High adoption of **Grade A** headers (62.3 average maturity) masks critical backend exposures.	**Control Imbalance:** Regulatory compliance focus on 'front-door' encryption often ignores administrative path isolation.
CHA (Charity)	**Extreme Fragility: 82.5%** of audited **charities** broadcast public-facing administrative gateways.	**Governance Vacuum:** Lack of technical **resource** leads to 'set-and-forget' deployments of legacy platforms.
EDU (Education)	**Identity Impersonation:** High **failure** rates in DMARC 'Reject' enforcement (**67%+** lack protection).	**Trust Dependency:** Over-reliance on 'Open' **academic** networks compromises research IP and student PII.
MAN (Mfg)	**Perimeter Fragility:** Lower-than-average maturity scores (**50.2**) with frequent legacy file leaks.	**Asset Sprawl:** Deep **supply** chains create 'Shadow Perimeters' where old vendor portals remain active and unpatched.
GEN (SME)	**Broadcast Vulnerability:** Significant 'broadcasting' of server tech and config data to any passive observer.	**Education Gap:** Business **owners** equate 'having a website' with 'being secure'.

Based on the **2026 UK Market Resilience Audit** data, we can identify distinct risk profiles for each sector. The data reveals a significant "Vulnerability Gap" where high maturity scores often fail to correlate with low exposure rates, particularly in the Charity and Education sectors.

FIN (Finance): The "Resilient but Leaky" Leader

Finance leads the market in **Maturity (65)** and maintains the lowest **Risk Area Score (30)**. However, its **42% Exposure Rate** is a concern for a highly regulated sector.

- **Key Finding:** Despite having the strongest defensive framework, the "Exposure Gap" suggests that legacy systems or complex third-party integrations are creating persistent "leaks" that maturity alone isn't solving.
- **2026 Context:** The highly regulated industry mindset is likely driving the high maturity, but the sector remains a primary target for sophisticated AI-driven identity attacks and perhaps needs a little more of a movement for further improvements.

CHA (Charity): The "High Risk Profile"

The Charity sector presents the most alarming data point. Despite a respectable Maturity Score (61), it faces a very high Risk Area Score (85) and a corresponding 82% Exposure Rate.

- **Key Finding:** This sector is in a "Compounding Risk Spiral." High maturity indicates they have the *policies* in place, but the sheer volume of high-risk data and exposed admin files suggests they are being overwhelmed by IT systems getting out of control along with a lack of investment.
- **2026 Context:** Recent findings suggest charities are increasingly targeted because they hold high-value donor data but often lack the specialised staff to maintain "active" defence across their entire digital footprint. There is a lot of help available to charities, either funded or offered pro-bono, charities perhaps need to better understand the help for risk remediation available.

EDU (Education): The "Monitoring Gap"

Education sits in the middle with a Maturity Score of 53, but its Exposure Rate (67%) is disproportionately high compared to its Risk Score (55).

- **Key Finding:** The data points to a failure in operational monitoring. The sector is likely "doing more with less," resulting in admin panels and files being left exposed even if the basic security infrastructure is "average."
- **2026 Context:** With budgets under extreme pressure, Education providers seem to be struggling to move from "passive" compliance to "active" threat hunting.

MAN (Mfg): The "Maturity Floor"

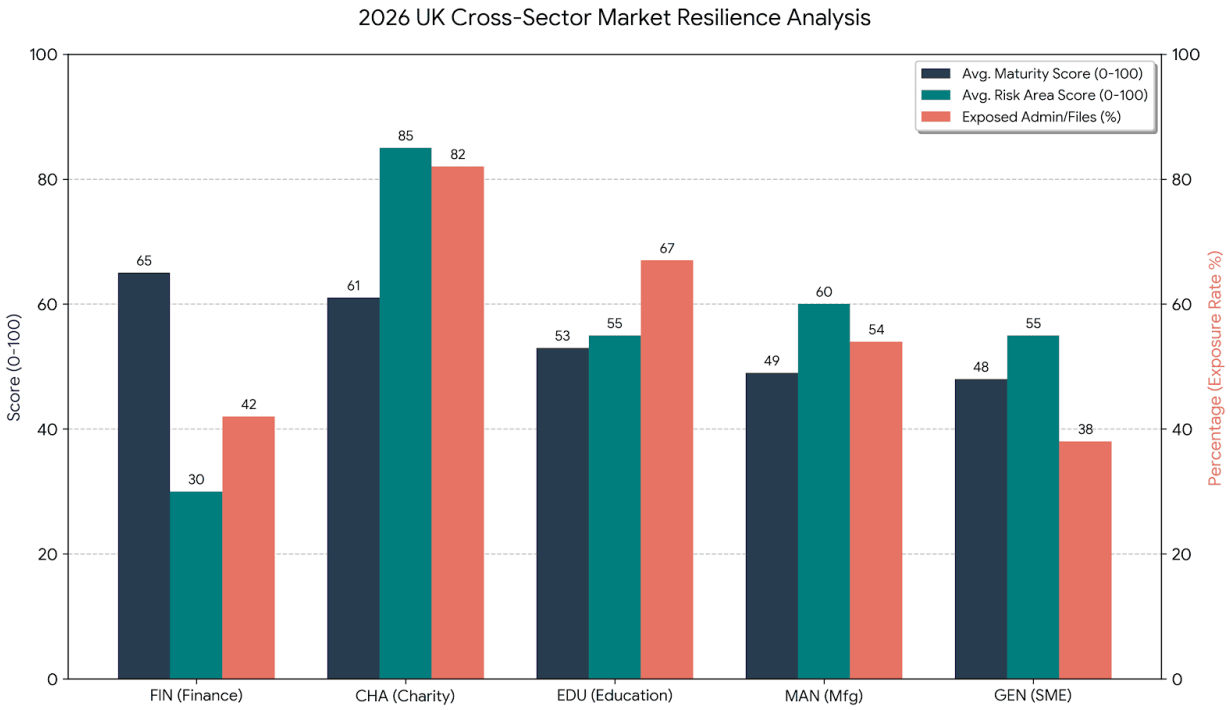
Manufacturing shows a low Maturity Score (49) and a high Risk Score (60), with a 54% Exposure Rate

- **Key Finding:** This sector is struggling with foundational resilience. The low maturity score suggests that Operational Technology (OT) and legacy manufacturing systems are dragging down the overall security posture, leaving more than half of their admin infrastructure exposed.
- **2026 Context:** As UK manufacturers "double down" on digital transformation in 2026, they are connecting older, unpatched systems to the web, significantly expanding their attack surface.

GEN (SME): The "Hidden Vulnerability"

SMEs have the lowest Maturity Score (48) but also the lowest Exposure Rate (38%).

- **Key Finding:** This is a "False Sense of Security" profile. The low exposure is likely due to a smaller digital footprint rather than better security. With the lowest maturity score, any increase in their "Risk Area" could lead to incident occurrence spiralling out of control.
- **2026 Context:** SMEs are currently the "testing ground" for automated AI phishing campaigns, where low maturity makes them easy targets for quick, high-volume breaches.



WHOLE MARKET Average Maturity: 55.2 | Risk Area:57.0 Exposed Admin Panels: 56.6

Closing Statement: The Remediation Gap

Following these findings, I sought to determine if these vulnerabilities were an unavoidable by-product of functional web architecture or the result of corner-cutting or oversight.

To test this, I initiated a project using a "standard delivery" WordPress site—a setup that mirrored the most frequent systemic failings identified in the audit. Using established industry best practices, I applied two different "hardening" techniques to the site. Both resulted in a move from a failing grade to a consistent **A+ rating**, achieved easily and within a very short timeframe, without sacrificing any site functionality.

This remediation reduced the site's observable risk profile by approximately 90%, demonstrating that many of the exposures identified are not inherently tied to technical limitations.

Instead, the findings suggest these risks may often relate to prioritisation, oversight, or resource constraints.

If a single consultant can harden a site to an A+ standard in a short timeframe, it raises an important question for the UK market: **why do these exposures persist at scale?**

