The Cyber Culture Clash Report:

Are UK Companies Hiding Behind Policies?

Contents

skillcast

Quick Summary from Skillcast's Cyber Culture Clash Index:

Skillcast analysed the largest businesses across eight key UK sectors to reveal a critical disconnect: how do cybersecurity policies measure up against real-world implementation? Which industries are walking the talk? Which are hiding behind impressive documentation? And which are operationally strong but underprepared on paper?

The findings:

- **Healthcare and pharmaceutical businesses excel operationally,** but their practice outpaces policy by 5:1 - a paradox that suggests strong execution could be masking weak governance frameworks that could prove brittle under evolving threats.
- **Financial services and retail demonstrate the tightest alignment,** with practice closely mirroring policy commitments - the gold standard for sustainable cybersecurity resilience.
- **Technology, manufacturing, and energy & utilities show the starkest gaps:** robust policies on paper fail to translate into practice, evidenced by escalating cyber attacks and implementation rates as low as 34%.
- **Public sector and government stands alone as the only sector experiencing a decline in reported cyber attacks year-on-year,** suggesting recent interventions may be taking effect.

Recent IBM research has found the average data breach now costs UK businesses £3.3 million - but financial damage is only part of the story. Breaches erode customer trust, can risk brand reputation, cause regulatory penalties, and can expose organisations to legal action.

When customer data is compromised, the ripple effects extend far beyond balance sheets, threatening the fundamental relationship between businesses and the people they serve.

What is the current status of the cybersecurity policies in the UK?

2025 has seen a huge wave of major cyber attacks. Some have crippled supply chains, others have forced large retailers offline for months, and even brought airport operations to a standstill.

Every day, huge companies across retail, transport, financial services - and even the public sector - are reporting that they're either under attack, or have just experienced one. These sophisticated cyber threats are costing businesses staggering amounts of money.

Take M&S, for example. A cyber attack earlier this year caused a significant data breach, forcing the company to pause all online orders in late April. The incident is now expected to reduce profits for the year by around £300 million. Sensitive information - names, contact details, payment details, and more - can be exposed, particularly when attackers target critical databases.

For Jaguar Land Rover, which experienced a supply-chain-hitting cyber attack in September, where more than a month's worth of worldwide production was lost, analysts have estimated its losses at £50m per week.

It feels like there's a new cyber attack every day, with JLR and M&S far from outliers. But how is this happening? When companies insist they're doing everything possible to protect themselves, why do attackers keep finding ways in, and why do these breaches continue to cause widespread disruption?

At the same time, we can't ignore the fact that compliance demands an investment of time and resources. Take training for instance – most professionals must complete at least 35 CPD hours per year, which could amount to significant time taken out of the office for conferences. Sometimes, just finding the right information from a library of resources and training materials can slow employees down and make compliance harder to achieve.

Skillcast's Cyber Culture Clash Index

When it comes to cybersecurity, what's written on paper often doesn't match what happens in practice.

That's why Skillcast has created the Cyber Culture Clash Index - an in-depth analysis of how UK organisations' stated cyber policies compare to their real-world performance.

The findings are concerning. Some of the UK's biggest companies publish lengthy, detailed cybersecurity policies, yet real-world incidents suggest that many may be hiding behind paperwork rather than building a genuine culture of cyber resilience.

In some cases, organisations score highly on policy strength but fail to translate this into meaningful action, neglecting to hire the right people, train staff to recognise phishing attempts, or monitor vulnerabilities within their supply chains.

Paper policies simply don't stop cyber attacks without the right compliance training.

Even industries that claim to have the most robust preventative measures on paper are falling short when it comes to implementation and behavioural change.

Why Cyber Culture Matters

Having a cybersecurity policy is one thing - enforcing it is another. Without consistent training, testing, and a robust incident response plan, employees remain vulnerable, sensitive data is at risk, and organisations face costly regulatory penalties.

Standards such as ISO 27001 outline best practices for safeguarding information, yet not every company applies them effectively or consistently.

Beyond compliance, a strong cyber culture builds brand trust and reputation. Demonstrating cyber resilience not only protects data - it protects credibility. In today's digital landscape, one incident can erode customer confidence overnight.

How the Cyber Culture Clash Index was created

To understand the gap between cybersecurity policy and practice, Skillcast analysed eight key data points across the UK's largest organisations, spanning eight major sectors - including financial services, energy and utilities, retail, and telecommunications.

Policy data points

The analysis first examined the strength and transparency of company policies by looking at points such as:

- Time since last privacy policy update (in months)
- Presence of a documented cybersecurity policy
- Whether the organisation confirms annual security testing
- References to ISO 27001, the international standard for Information Security Management Systems (ISMS)
- Cyber Essentials Plus certification, a UK government-backed standard involving a third-party technical audit to verify that essential cyber controls are effectively implemented

These policy-based indicators provided a foundation for understanding how well organisations communicate and maintain their commitment to cybersecurity on paper.

Practice data points

Next, Skillcast evaluated seven additional metrics that reflect the real-world execution of cyber resilience - the extent to which companies are actually putting their policies into practice. These included:

- Industry phishing rates
- Year-on-year change in cyber attacks reported to the ICO
- Percentage of businesses experiencing a cyber attack in the past 12 months (by sector)
- Proportion of organisations employing a Chief Information Security Officer (CISO) or Head of Cyber Security
- Percentage of staff working in security roles

Scoring and index

Each data point was assigned a weighted score out of 100, where a higher score indicates stronger preparedness and more actionable policies.

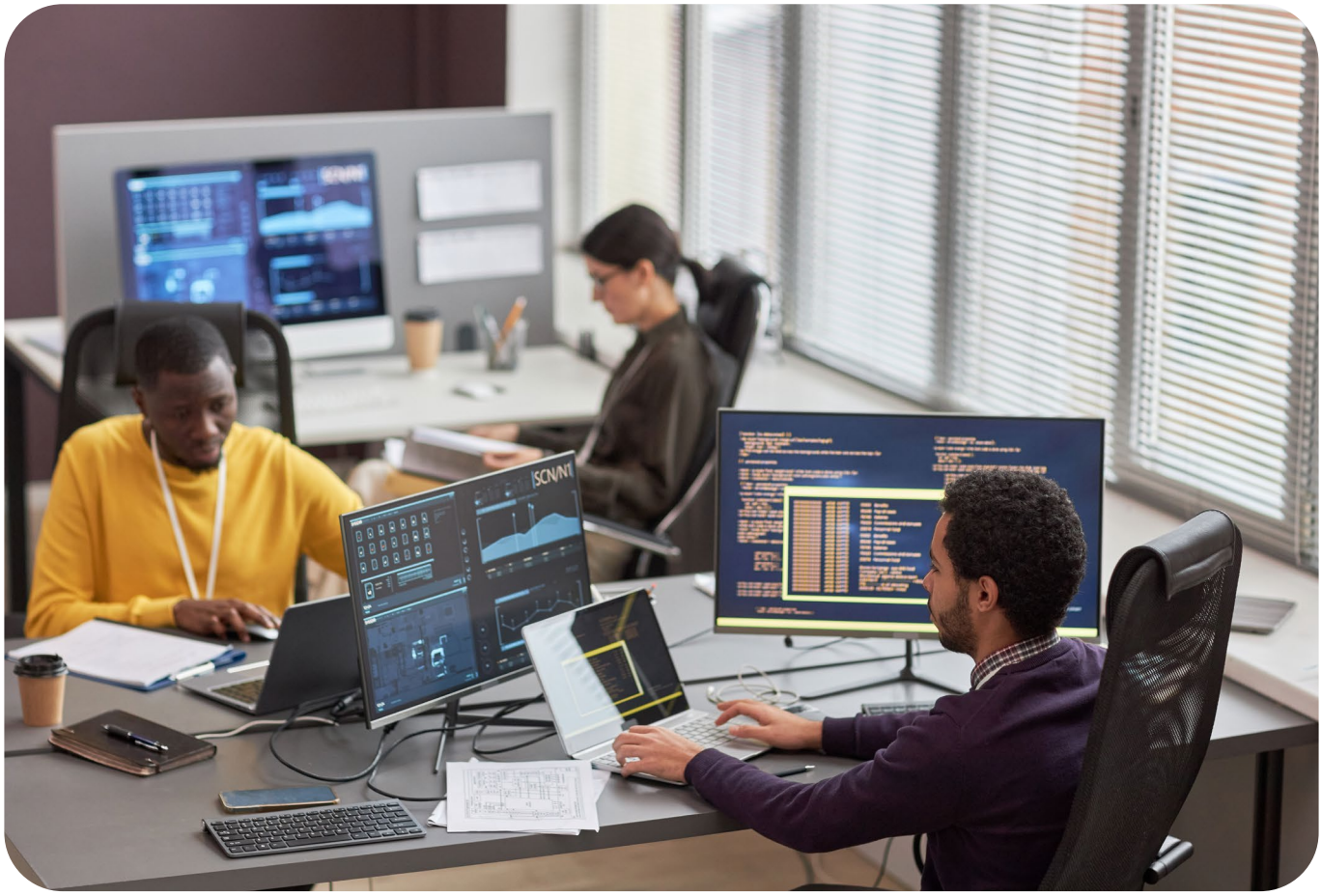
Skillcast then developed two composite measures - a policy score and a practice score - to assess the alignment between what companies say they do and what they actually do.

For **policy,** eight different data points were assessed. Each industry was scored on a scale of either 10 or 100 per data point, depending on the factor's relative importance to strong cybersecurity prevention. These were then combined to give each industry an overall score out of 260.

For **practice,** a further eight data points were evaluated. Here, businesses received weighted scores based on the number of reported cyberattacks, again producing an overall score out of 260.

Each industry was then given a ratio of how closely the policy matched performance, and reveal where practice is exceeding policy, and where there is a significant gap of under-implementation.

This approach provides a data-driven snapshot of how effectively UK companies are translating their cybersecurity promises into practice.



Skillcast's Cyber Culture Clash Industry Rankings

Industry	Policy	Practice	Practice ÷ Policy	Percentage aligned
Healthcare and pharmaceutical	18	93	5.17	19%
Retail and e-commerce	119	117	0.98	98%
Financial services	162	157	0.97	96%
Transportation and storage	124	118	0.95	95%
Public sector and government	193	152	0.79	79%
Manufacturing	114	79	0.69	69%
Energy and utilities	154	59	0.38	34%
Technology and SaaS provider	166	56	0.34	34%

An industry comparison

Cybersecurity challenges are not unique to any sector, but by comparing across industries, organisations can learn from high performers, and understand how to ensure policy matches implementation.

For boards and regulators, it provides crucial context for risk assessment and highlights where implementation failures pose the greatest threat to critical infrastructure and customer data.

Healthcare & Pharma: Operational strength is masking policy weakness

Practice vs Policy score - 5:1 (practice exceeds policy 5x)

Practice: 93 **Policy:** 18

Healthcare and pharmaceutical achieved the strongest practice-to-policy ratio at 5:1 but the high practice score shows a troubling paradox. The sector isn't necessarily excelling; rather, its documented policies are weak compared to operational reality. This inverted gap creates a dangerous illusion of success that could breed complacency.

The average healthcare business goes 31 months without updating its privacy policy, which could leave organisations vulnerable to evolving threats and regulatory drift. Only 20% maintain a documented cybersecurity policy, and not a single analysed organisation specifies maximum incident response time - a critical metric given the sensitivity of patient data and strict GDPR requirements.

Despite these policy shortcomings, healthcare experienced a relatively modest 37% increase in cyber attacks over two years - lower than most sectors. Employees manage an average of 71 passwords according to LastPass data, which shows that they're ensuring passwords are unique to reduce the chances of data breaches.

This presents a critical risk: stronger operational practices are currently compensating for weak governance frameworks. As cyber threats targeting healthcare supply chains and critical infrastructure intensify, this gap between informal practice and formal policy isn't sustainable. Without documented standards, incident protocols, and regularly updated frameworks, the sector's current resilience may prove dangerously brittle when facing sophisticated, evolving threats.

Retail - Keeping policies fresh and practice aligned

Practice vs Policy score - 1:1

Practice: 117 **Policy:** 119

Despite a number of high-profile attacks this year, the retail and e-commerce sector demonstrates some of the strongest alignment between policy and practice, showing that cybersecurity is being taken seriously - both on paper and in everyday operations.

Retail businesses had one of the best records for keeping their privacy policies up to date, averaging just 7.6 months since their last update. This suggests a regular review process and a proactive approach to governance - a stark contrast to the manufacturing sector, where policies were updated on average almost every three years (32 months).

Encouragingly, 7 in 10 retail organisations referenced ISO 27001, the global standard for information security management. This is particularly significant for a sector that has been frequently targeted through third-party vulnerabilities, such as compromised supply chains or payment systems.

At the leadership level, every retail and e-commerce business analysed (100%) had a designated Head of Cyber or CISO, signalling that accountability is clearly defined. And while high-profile breaches occasionally dominate headlines, the sector overall is performing well - with only 32% of retail companies reporting a cyber attack in the past 12 months, according to gov.uk data.

In practice, retail stands out as the most consistent performer when it comes to matching written policy with real-world execution. This balance between preparation and implementation suggests that retail organisations aren't just reacting to threats - they're evolving with them.

Financial Services - vigilance at the heart of economic security

Practice vs Policy score - 1:1

Practice: 162 **Policy:** 157

Financial services stands as one of the most critical sectors for maintaining cybersecurity vigilance and resilience. Housing millions of sensitive customer records and serving as the backbone of economic stability, a significant breach in this industry could trigger cascading failures across the entire financial system.

Given these stakes, FCA compliance training and robust cybersecurity protocols are non-negotiable. Yet our analysis reveals a nuanced picture: while financial services excels at documentation and governance structures, a subtle gap between policy ambition and operational execution persists.

The sector demonstrates several areas of genuine strength. Privacy policies are updated every six months on average - the most frequent refresh cycle of any industry analysed and a stark contrast to the 30+ month intervals seen elsewhere. This proactive approach to policy maintenance suggests a culture of regulatory awareness and adaptive governance.

Leadership commitment is exemplary: 100% of analysed businesses employ a dedicated CISO or Head of Cyber - a critical role for setting strategic direction, driving accountability, and embedding security throughout organisational culture. This universal adoption of senior cybersecurity leadership represents best-in-class governance.

The sector also experienced the lowest absolute number of cyber attacks and posted a 19% year-on-year increase in incidents reported to the ICO - still concerning, but notably more contained than the 30-50% increases seen in other industries.

However, beneath these strong metrics lies a potential complacency trap. Its Practice vs Policy ratio is almost at 1:1, but policy just outweighs practice. Yes, financial services nearly meets its stated commitments - but "nearly" may not be enough. The minor gap, while seemingly small, represents areas where documented standards aren't fully translated into daily operations. In a sector handling such sensitive data and facing increasingly sophisticated threat actors, even minor implementation gaps can become critical vulnerabilities.

Comprehensive cybersecurity training is crucial for financial services because human error remains the leading cause of breaches, with phishing attacks specifically targeting employees who hold access to high-value systems and sensitive customer data. Regulatory frameworks like FCA requirements also mandate ongoing staff education to maintain compliance, protect consumer trust, and demonstrate due diligence in safeguarding the financial infrastructure millions depend on daily.

Transportation & Storage - A steady alignment

Practice vs Policy score - 1:1

Practice: 118 **Policy:** 124

The transport and storage sector demonstrates one of the tightest policy-practice alignments at 95% - that shows an alignment between operational implementation and policy. However, this stability shouldn't breed complacency. High-profile incidents like the Heathrow attack prove how cyber breaches can halt operations instantly, creating ripple effects across the entire economy.

Despite strong alignment, both policy and practice scores remain among the lowest across all sectors analysed. Businesses update privacy policies every 19 months on average - infrequently enough to leave gaps in compliance. Only 50% maintain a dedicated cybersecurity policy, and just one business reported regularly updating security testing protocols.

The threat landscape is intensifying. ICO-reported incidents surged 33% over two years, with 35% of businesses experiencing an attack in the last 12 months alone. Critically, less than 1% of employees hold cybersecurity responsibilities - a dangerously thin line of defence for an industry where a single breach can ground flights, delay shipments, and disrupt supply chains nationwide.

Transportation's consistency is commendable, but low baseline scores reveal systemic underinvestment. As cyber threats grow in frequency and sophistication, the sector must elevate both policy ambition and operational capacity. Strengthened governance, dedicated security staffing, and regular testing aren't optional extras - they're essential safeguards for the critical infrastructure keeping Britain moving.

Public Sector & Government - Strong compliance, growing agility

Practice vs Policy score - 4:5

Practice: 152 **Policy:** 193

The public sector demonstrates the highest policy ambition of any sector at 193, proving that compliance isn't merely aspirational - it's embedded into operational DNA. Operating under strict regulatory and procedural frameworks, government organisations show clear discipline in translating policy into practice, achieving 79% implementation.

Most remarkably, the public sector stands alone as the only industry recording a decline in cyber attacks reported to the ICO - down an impressive 77% over two years. While some of this may reflect threat actors pivoting toward more lucrative private-sector targets, it also signals genuine progress following high-profile incidents like the devastating NHS attack, which catalysed sector-wide security improvements.

The sector also leads on human resilience, recording the lowest phishing click rates across all industries - clear evidence that compliance training and employee awareness programmes are delivering measurable impact.

Despite these strengths, the 21-point implementation gap suggests room for improvement. Public bodies excel at establishing frameworks, but maintaining agility as threats evolve remains a challenge. Policies must keep pace with rapidly shifting attack vectors - what's compliant today may be inadequate tomorrow.

The public sector is successfully transforming compliance culture into genuine cyber maturity. The challenge now is sustaining that momentum: ensuring processes remain not just compliant, but continuously adaptive, responsive, and resilient against emerging threats targeting the critical services millions depend on.

Manufacturing is lagging behind in cyber resilience

Practice vs Policy score - 7:10

Practice: 79 **Policy:** 114

The manufacturing sector faces significant challenges in aligning policy with practice, making it one of the lowest-performing industries in the Cyber Culture

One major concern is policy maintenance. Manufacturing companies had the longest average time since privacy policy updates at 32 months, a red flag that governance and risk management may not be keeping pace with evolving cyber threats. Only 33% of businesses analysed had a formal cybersecurity policy, highlighting a gap between intentions and actionable frameworks.

While 60% of manufacturers reference ISO 27001, which is encouraging for an industry dependent on complex supply chains, only 20% hold Cyber Essentials Plus certification. This indicates that formal assurance and verification processes are still limited, leaving companies potentially exposed.

These weaknesses are reflected in practice: the sector saw a 51% increase in businesses reporting cyber attacks to the ICO, and a mere 1.9% of staff in these companies are dedicated to cybersecurity roles. Combined, this suggests that manufacturing firms may be understaffed, underprepared, and overexposed relative to the cyber threats they face.

In short, manufacturing shows a clear policy and practice gap. Strengthening governance, increasing dedicated cyber staff, and formalising security controls are critical steps if the sector is to reduce vulnerabilities and build true cyber resilience.

Energy & Utilities: Exposed at the core

Practice vs Policy score - 2:5

Practice: 59 **Policy:** 154

The energy and utilities sector shows the widest gap between cyber policy and practical implementation of any industry analysed- achieving just 38% alignment. This disconnect exposes dangerous vulnerabilities within critical infrastructure that millions rely on every day.

The governance shortfall is stark. Energy and utilities recorded the fewest organisations with a dedicated CISO or Head of Cyber, highlighting a lack of senior accountability for security strategy. Almost half of all businesses in the sector experienced a cyber attack in the past 12 months, with even major players like BP and Shell hit multiple times.

Reports of cyber attacks to the ICO have surged by 71% over two years - the steepest rise across all industries. This acceleration is especially concerning given the sector's reliance on interconnected systems, extensive customer data, and its role in national infrastructure.

Human behaviour adds another layer of risk. Phishing click rates reached 41%, among the highest of any sector, underscoring how employee awareness and training lag behind both policy and threat evolution.

In short, the energy and utilities sector faces a critical cyber resilience challenge - one that demands urgent investment in leadership, governance, and workforce readiness to protect the systems that keep society running.

Energy infrastructure represents a prime target for state-sponsored actors and ransomware groups, with attacks capable of cascading into widespread service disruptions. The widening gap between documented policies and operational reality leaves critical systems dangerously exposed at precisely the moment when threats are accelerating.

Technology and SaaS - strong policies, weak practice

Practice vs Policy score - 1:3

Practice: 56 **Policy:** 166

Despite being home to some of the most cyber-aware organisations, the technology and SaaS sector shows the weakest alignment between policy and practice in the Cyber Culture Clash Index. With implementation lagging behind significantly, the data suggests that while tech companies are writing robust policies, many are struggling to translate them into consistent, real-world action.

This "policy-first" culture may reflect the sector's focus on compliance and frameworks over day-to-day execution. The industry scored 166 for policy but just 56 for practice, the lowest of all sectors analysed. This imbalance indicates a maturity gap: policies are in place, but they're not yet being lived across the organisation.

The findings reveal a mix of preparedness and exposure. Technology and SaaS firms employ the largest proportion of cybersecurity professionals, with 8% of staff in security roles in more than double any other industry -- and reported the highest number of passwords per employee, signalling high awareness. Yet these strengths aren't preventing breaches: 69% of companies reported a cyber attack in the past year, the highest rate of any sector.

This contradiction highlights a critical problem - having the right policies on paper isn't enough. Without embedding them into behaviour, even highly skilled teams remain vulnerable.

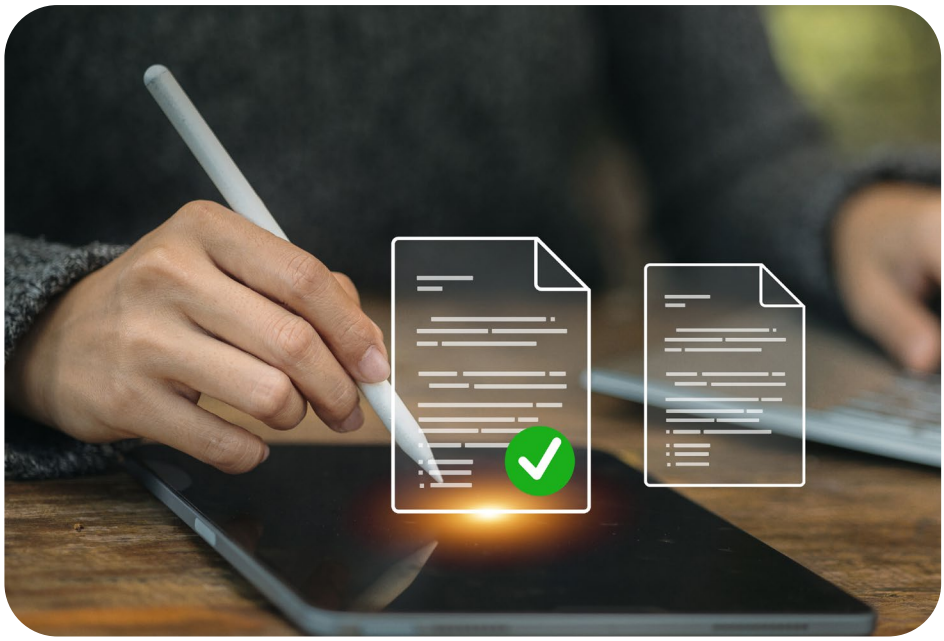
Encouragingly, technology firms referenced cybersecurity more often in their annual reports than any other sector, demonstrating that the issue is firmly on the strategic agenda. The next challenge is to ensure that practice catches up with policy, turning ambition into measurable resilience.

Why the gap matters

Key cybersecurity takeaways for organisations

Cybersecurity is not a box-ticking exercise. A well-written policy without consistent, practical execution leaves organisations exposed to breaches, financial penalties, and lasting reputational harm. True resilience depends on alignment between what's written and what's done.

- **Audit your practice, not just your policy.**
  The biggest vulnerabilities often lie in execution. Regularly test how well policies translate into real-world behaviour.
- **Look beyond compliance.**
  Meeting minimum standards is no longer enough in a fast-evolving threat landscape. Aim for continuous improvement, not just regulatory alignment.
- **Balance policy with action.**
  Overemphasising documentation can create a false sense of security. Ensure written controls are actively embedded in daily operations.
- **Invest in frontline implementation.**
  Cybersecurity training, monitoring, and enforcement must match the ambition of your governance frameworks. Cyber resilience is built through people and practice, not paperwork.



Recommendations: Closing the cyber culture gap

To reduce the gap between policy and practice and strengthen overall cyber resilience, organisations should focus on the following:

- **Conduct regular, transparent security testing**
  Ensure all systems are routinely tested and results are visible to relevant stakeholders, creating accountability and uncovering vulnerabilities before they escalate.
- **Set and communicate clear incident response times**
  Define maximum response times for cyber incidents and make these expectations transparent across the organisation to improve cybersecurity awareness.
- **Embed ISO 27001 standards into everyday operations**
  Integrate international information security standards into daily workflows to move beyond compliance and build a culture of continuous protection.
- **Provide continuous cybersecurity training for employees**
  Equip staff at all levels with up-to-date knowledge and practical skills to recognise and respond to cyber threats, reinforcing policy through action.
- **Update privacy policies consistently**
  Maintain current and accurate privacy policies, ensuring they reflect evolving risks and regulatory requirements while demonstrating organisational accountability.

The Cyber Culture Clash Index shows a clear pattern: policy alone does not guarantee protection. Only a culture of cyber awareness, training, and accountability can defend against the rising tide of cyber threats.

Companies must move beyond paperwork and invest in cybersecurity awareness training.

Methodology

Skillcast analysed 80 of the largest UK businesses in healthcare and pharmaceutical; retail and ecommerce; financial services; transportation and storage; public sector and governance; manufacturing; energy and utilities and technology and SaaS providers.

To understand policy, Skillcast looked at: average number of mentions of cybersecurity in their annual reports; the average number of months since each privacy policy was updated; the number of businesses with a cyber security policy; average number of sections covering different security areas in the policy; number of businesses that announce they annually update security testing; number of businesses that outline a maximum incidence response time; number of businesses that outline ISO 27001; and the number of businesses registered as Plus on Cyber Essentials.

To understand practice, Skillcast looked at: the number of businesses with a CISO or Head of Cyber; the % of businesses that have experienced a cyber attack in the last 12 months, by sector; the increase in cyber attacks reported to the ICO in the last two years, by sector; security staff ratio; average number of passwords per employee, by industry; and industry phishing click rates for enterprises.

Each industry was given a weighted index score next to each data point, and a ratio was then given, with extra weighting given to the businesses that had the fewest cyber attacks, to show how practice matches up to policy.

skillcast

About Skillcast

Skillcast helps companies build ethical, inclusive and resilient workplaces. It provides content and technology to digitise and streamline compliance processes and manage them from a single compliance portal. Its product range includes a Learning Management System with comprehensive off-the-shelf compliance course libraries, a Policy Hub, Staff declarations, Anonymous surveys, CPD tracking, and Compliance registers for gifts, expenses, PA dealing, and whistleblowing.

To start your free trial

Call us on +44 20 7929 5000

Visit www.skillcast.com/free-trial

Or scan the QR code below