



# 12 Cyber Challenges UK SMEs Face Right Now with Fixes That Work



UK businesses are facing unprecedented cyber risk. In the past year, **cyberhackers cost UK SMES £3.4 billion.**

What can UK SMEs do to fight back?



## 01 RISING CYBER THREATS

-  **Risk:** Phishing, ransomware, and automated attacks are accelerating. In 2024, UK businesses experienced an average of over **753,000 malicious breach attempts per business**, and attacks occurred approximately every **42 seconds**.
-  **Solution:** Kickstart with **Cyber Risk Assessments** to catch weak spots early, prioritise remediations, and shore up defences before attackers exploit them. After the Cyber Risk Assessment, organisations should create a strategy to close the risks.



## 02 COMPLEX REGULATIONS

-  **Risk:** With GDPR, NIS2, and emerging UK laws, **27% of businesses reported being hit by a cyber-attack in the past year** and even more expect disruption soon.
-  **Solution:** Engage **Compliance Advisory Services** to decode the complexity, stay ahead of changes, and avoid fines and PR damage.



## 03 UNCLEAR POLICIES & HUMAN ERROR

-  **Risk:** Human mistakes are still a major breach vector. In the UK, **84% of businesses reporting breaches** said phishing was involved.
-  **Solution:** Establish **clear, practicable Policies & Standards** and reinforce them across the team to reduce confusion and mistakes.



## 04 WEAK SECURITY STRATEGY

-  **Risk:** Rising threats with no consistent plan leaves businesses dangerously exposed — especially with **35% of SMEs suffering cyber incidents in the past year**, many with no maturity roadmap.
-  **Solution:** Conduct **Maturity Assessments**. They help align your security posture with growth plans and build a long-term resilience roadmap.



## 05 SUPPLY CHAIN RISKS

-  **Risk:** Third parties are now major entry points for attackers. While detailed numbers in the UK vary, across businesses, **50% experienced some form of breach** and they are often through vendor systems.
-  **Solution:** Understand 3<sup>rd</sup> party exposure, associated risks and define approach for how to assure suppliers and 3<sup>rd</sup> parties.



## 06 UNTESTED DEFENCES

-  **Risk:** Many businesses feel “safe” until they’re tested by attackers. In 2024, phishing was found in **84% of breach incidents**, showing defensive gaps.
-  **Solution:** Validate your posture with **Penetration Testing, BAS (Breach & Attack Simulation), and Cyber War-Gaming**.



## 07 INSECURE APPLICATIONS

-  **Risk:** Web/app vulnerabilities remain a major problem. Limited UK-specific figures — but globally, many data breaches stem from insecure software.
-  **Solution:** Add **Secure Code Reviews** into your release lifecycle and catch flaws early. Understand security posture of platforms, hardware and software. Deploy mechanisms for secure posture management.



## 08 PRIVACY GAPS

-  **Risk:** The ICO recorded **3,000+ data breaches** in 2023 where personal data was at risk. The retail, finance, and education sectors were the most affected.
-  **Solution:** Use **Data Protection & Privacy Advisory** services to strengthen your privacy practices and build trust.



## 09 SENSITIVE DATA LEAKAGE

-  **Risk:** Insider mistakes and misconfigurations can be damaging. UK businesses report **financial and reputational fallout** from data breaches all the time.
-  **Solution:** Stop leaks with **Data Loss Prevention (DLP)**, safeguarding data across email, endpoints, and the cloud. Define information asset handling approach and deploy supporting technology to assure requirements.



## 10 HUMAN ERROR & LOW AWARENESS

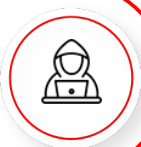
-  **Risk:** Employee awareness remains low. **84% of reporting businesses** were victims of phishing. And only a minority implement regular training.
-  **Solution:** Launch **Security Awareness Programmes** that train staff on real risks and reduce risky behaviour.

## 11 NO CONTINUITY PLANNING

-  **Risk:** Attacks disrupt operations. One study warned that victims faced **£44 billion in losses over five years**, and only half of businesses have tested recovery plans.
-  **Solution:** Build resilience with **BC/DR Planning** so operations can continue despite disruptions.

## 12 BACKUP FAILURES

-  **Risk:** Backups fail when badly configured or untested and even high-profile organizations suffer downtime due to data loss.
-  **Solution:** Implement **Backup & Recovery Assurance** by running regular restoration tests and verifying backup integrity.



### Punchline

UK SMEs aren't powerless but inaction is costly. SysGroup helps you turn risk into resilience with services that are practical, affordable, and business-focused.