



Discover how Cyberfort
Penetration Services helped
a UK consumer organisation
to maintain the security,
integrity and availability of its
digital platforms

Industry:
Retail &
Consumer

Location:
United Kingdom

Introduction

In this case study we cover why a highly respected UK consumer organisation that manages significant volumes of consumer, membership, subscription, and digital service data chose Cyberfort as its Penetration Testing partner. The organisation in this case study is a trusted brand that provides online services, product reviews, legal support, and consumer advice to millions of users.

Maintaining the security, integrity, and availability of its digital platforms is critical. The organisation must protect sensitive personal information, defend against evolving cyber threats, and maintain the trust and confidence of its members while ensuring compliance with relevant data protection and security requirements.

The Challenge

The organisation required a specialist penetration testing partner capable of delivering high-quality security assessments within challenging timescales to ensure all testing activities were completed before the end of its financial year. As a leading UK consumer organisation, it relies heavily on its digital platforms and online services to deliver trusted advice, product reviews, subscription services, and member support. Protecting these services is critical to maintaining member trust and safeguarding sensitive customer and business information.

The Solution

Cyberfort has partnered with this customer for several years, providing a comprehensive programme of penetration testing and security assurance services across its critical infrastructure, end-user environments, and customer-facing platforms.

Working closely with the customers internal teams, Cyberfort delivered flexible and scalable testing services aligned to project deadlines and evolving business priorities. This enabled the customer to gain independent assurance over the security of its systems and applications while ensuring testing activities were completed within demanding timescales.

By combining experienced CREST-qualified consultants, proven methodologies, and timely reporting, Cyberfort provided the customer with actionable security insights and prioritised recommendations. This enabled the organisation to address identified vulnerabilities efficiently, improve its overall security posture, and maintain confidence in the security of its digital services and business operations.

This approach ensured that the consumer organisation could meet its testing objectives within the required timeframe while benefiting from a trusted security partner capable of delivering both technical expertise and operational flexibility.

The engagement included:



- External Network Foot-Printing Assessment
- Internal Network Scanning and Internal Network Infrastructure Assessment
- Web application assessment of the company website
- Cloud Configuration Reviews
- Workstation Build Review
- Ransomware Readiness Assessment



The Outcome

Through a collaborative and transparent approach, Cyberfort and the consumer organisation established clear communication channels throughout the engagement, enabling vulnerabilities to be quickly reviewed, prioritised, remediated, and retested. This provided the customer with confidence that identified security weaknesses had been effectively addressed and validated through independent verification.

The engagement enabled the consumer organisation to maintain confidence in the security of its key business systems and online services while supporting a culture of continuous security improvement through regular testing, remediation, and validation activities.

As a result, they benefited from:



- Faster remediation and verification of identified vulnerabilities.
- Improved visibility of security risks across critical systems and applications.
- Independent assurance that remediation activities had been successfully completed.
- Enhanced resilience against evolving cyber threats, including ransomware and attacks targeting customer-facing services.
- Strengthened security controls across its infrastructure, end-user environments, and digital platforms.
- A flexible, trusted security partnership capable of supporting changing business priorities and challenging delivery timescales.