CASE STUDY

How a UK Firm Strengthened Its Cyber Security Posture in 90 Days

Chapman Technology Partners

Overview

A mid-sized UK professional services organisation approached Chapman Technology Partners to gain a clearer understanding of its cyber security posture. Operating in a sector where client data, contractual obligations and investor confidence are critical, the firm wanted assurance that its systems, staff and cloud environments were secure — and aligned with UK regulatory expectations.

Chapman Technology Partners completed a full Cyber Risk Assessment, providing the leadership team with detailed insight into vulnerabilities, human risk, cloud misconfigurations and operational weaknesses. The assessment uncovered several high-impact risks that, if left unresolved, could have led to data breaches, compliance failures or business interruption.

(All details in this case study are anonymised and summarised to protect the confidentiality of the client.)

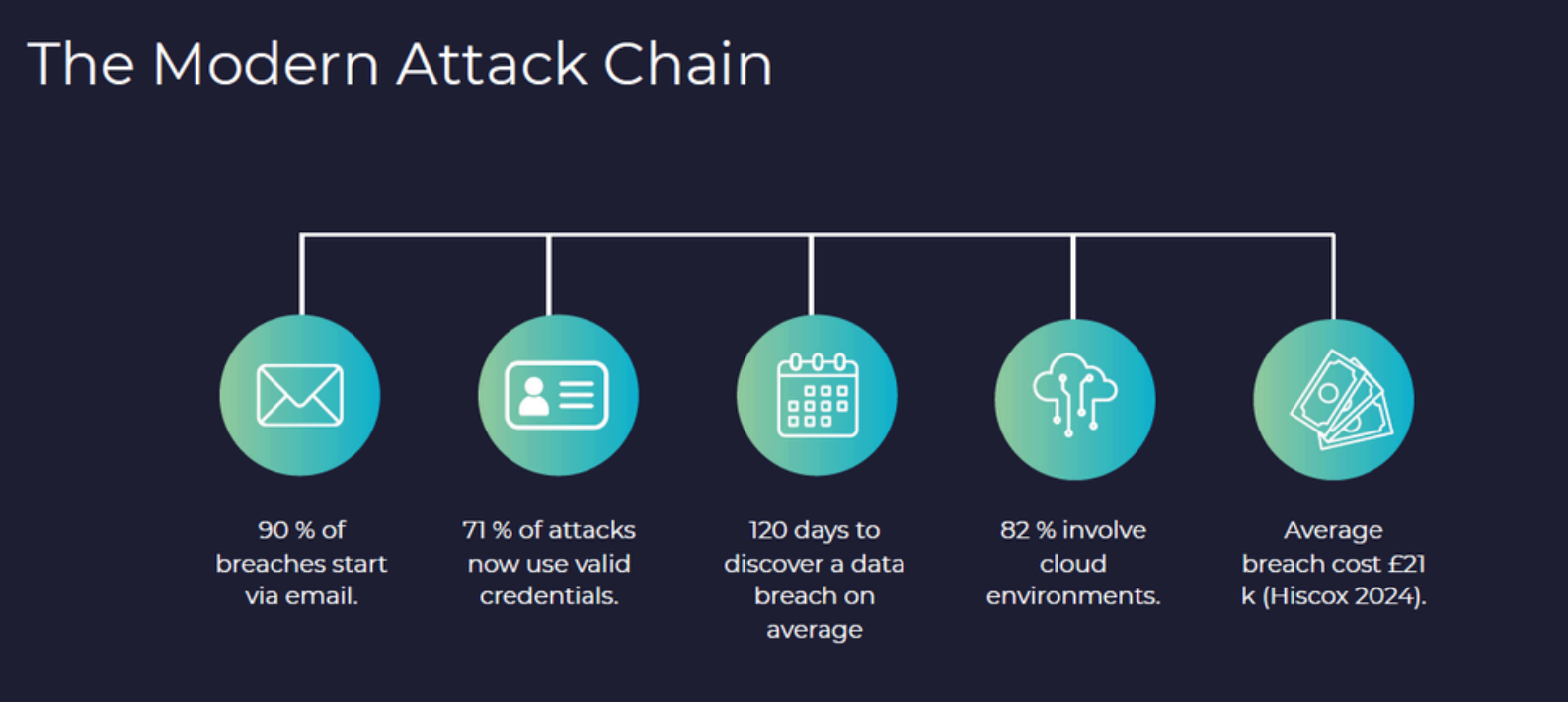
Overview

The organisation had grown rapidly and, like many scale-up and professional services businesses, technology controls hadn't kept pace with the increased volume of client data, distributed work, and reliance on cloud systems.

The firm's objectives were clear:

- Understand exactly where cyber risks existed
- Assess exposure across people, devices, data and cloud services
- Validate whether internal policies matched real-world practice
- Identify gaps that cyber insurance might not cover
- Build resilience and ensure readiness for audits or investor due diligence

The leadership team wanted evidence — not assumptions — so the business could make informed decisions.



Our Approach

Chapman Technology Partners deployed a structured, evidence-led Cyber Risk Assessment covering:

1. Human Risk & Behaviour Analysis
Phishing simulations, credential hygiene checks, and behavioural insights.

2. Cloud Security & Microsoft 365 Review
Secure Score, authentication controls, mailbox protections, data governance.

3. Dark Web Intelligence Scanning
Identification of compromised credentials from historic breaches.

4. Endpoint & Device Security Audit
OS security, vulnerabilities, encryption and patch management.

5. Identity & Access Threat Analysis
Tracking failed logins, geographic access attempts and privilege misuse.

6. Compliance & Governance Review
Alignment with Cyber Essentials and regulatory best practice.

7. Reporting & Remediation Roadmap
Regulator-ready documentation and a structured 90-day improvement plan.

Key Findings

1. Human Risk Exposed the Greatest Attack Surface
Across seven simulations, 86% opened emails, 14% clicked, and 8% submitted credentials — demonstrating high susceptibility to real-world phishing attacks.

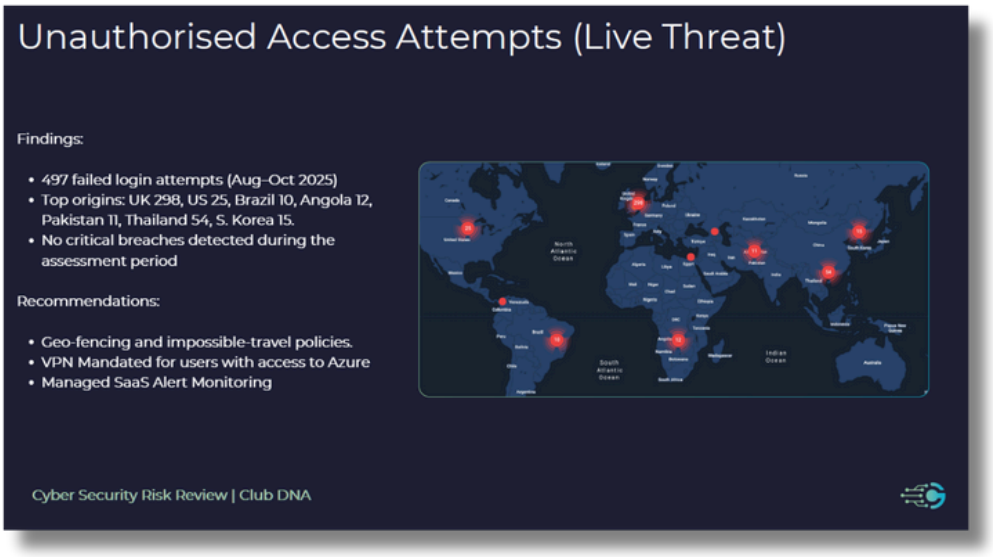
Impact: Attackers could have gained valid login details — a key contributor to modern breaches.

2. Compromised Credentials Found on the Dark Web
Multiple historic logins associated with staff accounts were found circulating on dark-web marketplaces.

Impact: Password reuse could have enabled attackers to access cloud systems using stolen credentials.

3. 497 Unauthorised Login Attempts Detected
Over a three-month period, almost 500 failed access attempts originated from multiple countries including the UK, US, Brazil and Thailand.

Impact: Demonstrates active attempts to compromise accounts via brute force, credential stuffing or reconnaissance.



4. Device Security Was Not Fit for a Regulated Environment
Findings included:

- Devices running Windows Home (no business security features)
- Zero encryption across laptops handling sensitive data
- Multiple critical vulnerabilities, including a high-severity SQL Server Management Studio flaw

Impact: Lost or stolen devices could have resulted in data breaches, reportable under UK GDPR.

5. Sensitive Data Stored Locally on Endpoints
The scan identified 7,371 PII files across devices, representing an estimated £41,395 data-risk exposure.

Impact: Increased exposure to data leakage, regulatory scrutiny and financial penalties.

6. Microsoft 365 Security Was Below Baseline
The organisation had a 39.34% Secure Score, with several missing or misconfigured security controls.

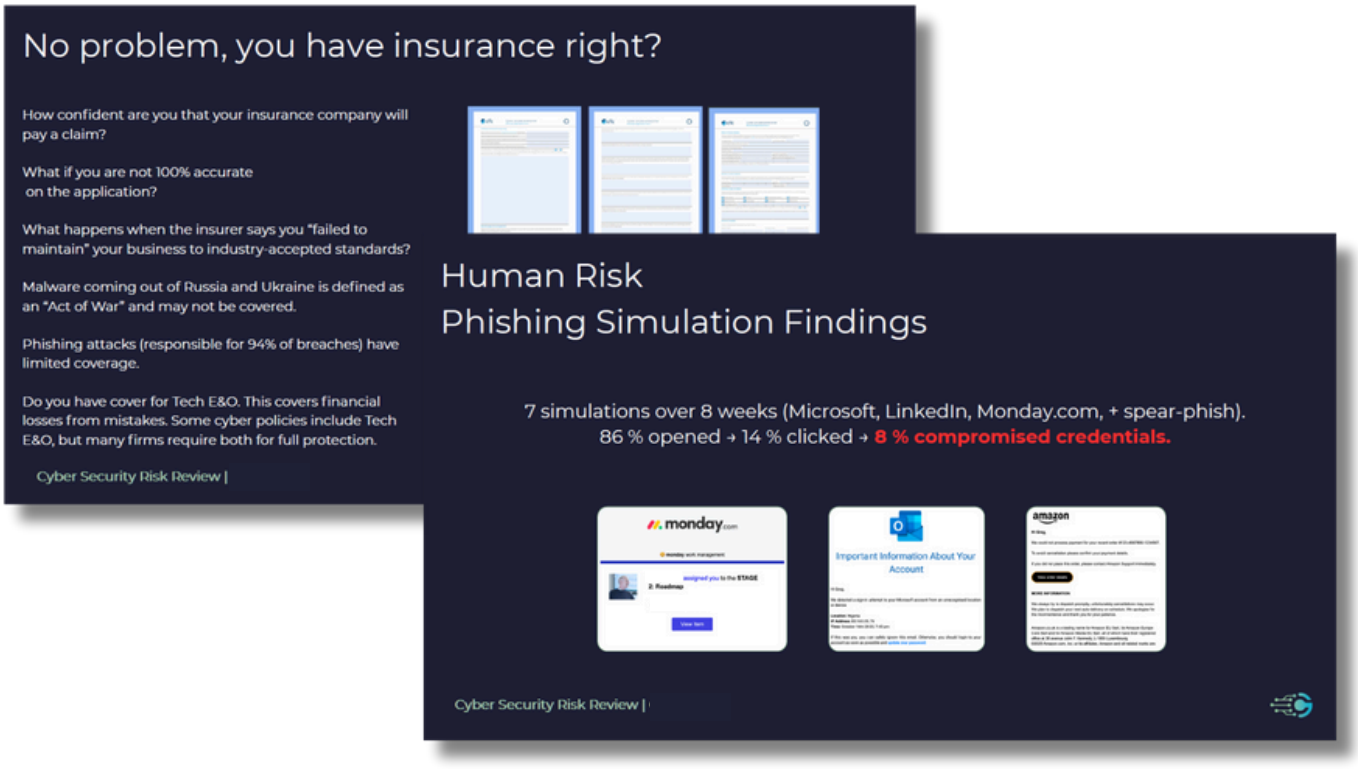
Risks included:

- Legacy authentication still active
- Missing mailbox auditing
- Inactive sessions left open
- No daily backup of mailboxes or SharePoint

Impact: Increased likelihood of account compromise and data loss.

7. Email Authentication Was Weak
SPF, DKIM and DMARC records were missing or misconfigured across domains.

Impact: Attackers could easily spoof emails, damaging brand reputation and enabling convincing phishing attacks.



The Solution

Chapman Technology Partners delivered a structured, prioritised roadmap aligned with Cyber Essentials and modern cloud security expectations.

Immediate Actions

- Enforce MFA and Conditional Access
- Block legacy authentication
- Patch critical endpoint vulnerabilities
- Begin endpoint encryption rollout
- Implement email authentication (DMARC/DKIM/SPF)

30-Day Milestones

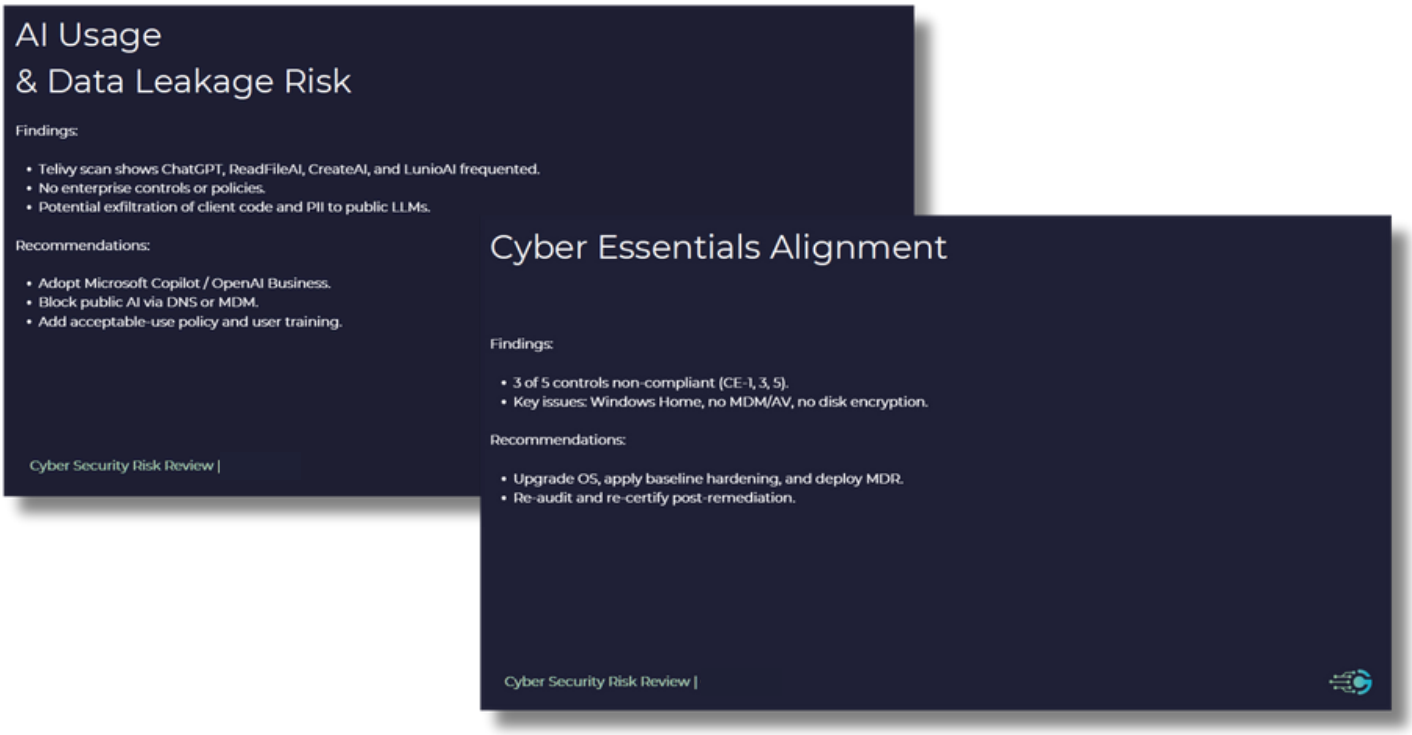
- Deploy Intune for device management
- Introduce centralised data governance
- Roll out password manager and phishing reporting tools

60-Day Milestones

- Apply advanced email security
- Introduce monthly phishing simulations
- Configure automated cloud backups

90-Day Outcomes

- Secure Score uplift benchmarked
- Compliance alignment reassessed
- Full staff awareness training programme launched



Impact & Results

Within 90 days, the firm achieved:

✓ **Significant uplift in Microsoft Secure Score**
Reducing account compromise risk.

✓ **Full encryption of devices**
Ensuring laptops could no longer cause data breaches if lost or stolen.

✓ **Reduced human-risk exposure**
Through training, simulations and better reporting tools.

✓ **Improved email deliverability and brand protection**
With correct authentication records.

✓ **Strengthened compliance position**
Supporting Cyber Essentials, operational resilience obligations and audit readiness.

✓ **Clear evidence for leadership, partners and stakeholders**
Giving the firm confidence in its cyber maturity.

> "This assessment gave the organisation absolute clarity. They could finally see where risk lived, how attackers could exploit it, and what needed to happen to protect their people, clients and reputation. Within 90 days, their security posture was transformed."
>
> **Greg Chapman**
> **MD, Chapman Technology Partners**

Conclusion

This case demonstrates the value of a structured Cyber Security Risk Assessment for businesses operating in regulated or data-sensitive environments.
It provides leadership with the truth: a clear, evidence-based understanding of vulnerabilities — and a practical roadmap to fix them quickly.

Ready to Strengthen Your Firm?

Book a Cyber Risk Assessment today.

www.ChapmanTechnologyPartners.co.uk

Chapman Technology Partners

Strategic IT, Cyber Security & AI Solutions
for Regulated Firms

Strawberry Fields Digital Hub,
Chorley, PR7 1PS

enquiries@ctpartners.co.uk
01257 542388

CYBER ESSENTIALS
CERTIFIED