CYBERSECURITY & IRM

CASESTUDY

Secure growth for SME lending: cyber resilience engineered ahead of the threat

Background

A UK-authorised bank ("the Client") operates as a digital-native lender to small and-medium enterprises (SMEs). It underwrites working-capital lines, equipment-finance, and merchant-cash-advance products entirely through APIs that ingest Open Banking data and realtime accounting-platform feeds (e.g., Xero, QuickBooks). With £12 billion in assets and 250 000 active SME borrowers, the cloud-only stack and 24/7 self-serve portal drove 35% compound growth—yet also broadened the cyber attack surface. Board concern intensified after a sector-wide ransomware wave and the PRA/FCA's sharpened Operational Resilience expectations.

Introduction

Enigma Risk Advisory, advised in a six-month Cybersecurity Risk Assessment & Strategy engagement that:

- Bench-marked cyber maturity against ISO 27001:2022, National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) v2, PRA/FCA PS21/3, and forthcoming Digital Operational Resilience Act (DORA) requirements for EU-facing services.
- Quantified loss exposure via AI-driven attack-path modelling and stochastic simulations.
- Crafted a target-state strategy—spanning AI-based pre-emptive defence, vulnerability eradication, incident-response orchestration, and culture uplift—tied to the bank's SME-growth roadmap

Challenges Faced

Domain	Key Pain-Point	Risk Implication
Threat Detection	Legacy SIEM flooded analysts with 72,000 daily alerts; 10 hour mean-time-to-detect (MTTD)	High attacker dwell-time → greater loss severity
AI & ML Utilisation	ML confined to credit-risk scoring; no autonomous threat hunting or incident triage	Slow containment, talent bottlenecks
Attack Surface	160 public APIs (loan origination, open-banking, partner marketplaces) & multi-cloud SaaS	Misconfigurations and shadow IT expand entry points
Third-Party Risk	34 fintech partners process PII & loan-book data	PRA/FCA and GDPR breach liability; DORA vendor-risk gaps
Culture & Governance	Security viewed as "tech back-office"; 26% phishing-test failure rate	Weak human firewall, regulator scrutiny
Compliance Landscape	Overlapping PRA/FCA Operational Resilience, NIS Regulations, ISO 27001:2022, Cyber Essentials Plus, DORA	Audit fatigue, fragmented evidence collection

CYBERSECURITY & IRM

CASESTUDY

Secure growth for SME lending: cyber resilience engineered ahead of the threat

Results and Impact

- MTTD collapsed from 10 hour to 27 min, while mean-time-to-respond (MTTR) fell 52% after deploying AI-powered XDR and SOAR.
- External attack surface reduced 39% by decommissioning orphan APIs, enforcing zero-trust segmentation, and auto-hardening S3 buckets.
- £9.6 million annual risk-adjusted loss avoided (validated in ICAAP) thanks to proactive control uplift.
- Staff cyber-awareness score increased +41 percentage points; phishing-fail rate dropped to 5%.
- Zero material findings in a PRA Section 166 tech-risk review; Cyber Essentials Plus achieved in seven weeks.

Solutions Implemented

a. AI-Enabled Threat-Lifecycle Defence

- Pre-emptive detection – Graph-based ML revealed kill-chain anomalies across SaaS, endpoint, and cloud-native logs.
- Autonomous containment – SOAR runbooks isolated compromised Kubernetes pods; an LLM assistant drafted incident tickets, regulator notifications, and root-cause summaries.

b. Vulnerability & Attack-Surface Management

- Continuous external scanning with ML ranking Common Vulnerabilities and Exposures (CVEs) by exploit likelihood and loan-book impact.
- Infrastructure-as-Code policy gates (OPA) blocked deployments violating CIS benchmarks.

c. Regulatory-Aligned Control Framework

- Unified library mapping ISO 27001 controls, NIST CSF functions, PRA/FCA impact tolerances, and DORA ICT-risk articles.
- Evidence captured automatically via API hooks into IaC repos, ticketing, and KMS—cutting audit-prep effort 60%.

d. Culture & Capability Programme

- Quarterly Purple-Team Game-Days—LLM-guided red-team emulating ransomware vs. blue-team SOAR response; lessons fed into skills matrix.
- Slack-delivered micro-learning and adaptive phishing powered by reinforcement learning focused on high-risk cohorts.

e. Quantitative Cyber-Risk Model

- Frequency-severity model calibrated with FS-ISAC & Verizon DBIR data; outputs informed capital buffering and cyber-insurance purchase decisions.

Conclusion

Integrating AI-driven threat analytics, rigorous vulnerability reduction, and culture-first governance under a single, regulator-aligned framework transformed the bank's cyber posture from reactive compliance to proactive resilience. The strategy protects its digital SME-lender mission, satisfies PRA/FCA and upcoming DORA expectations, and positions the bank as a benchmark for cyber maturity among UK fintech lenders.