CONFIDENTIAL

Barclays PLC

Cybersecurity Program Summary

Risk Management, Strategy & Governance | Based on Barclays PLC Annual Report 2025

Report Date: May 07, 2026 | LSE: BARC | NYSE: BCS | Banking & Financial Services | England, UK

This document summarizes Barclays PLC's cybersecurity risk management strategy, program structure, governance framework, and resilience posture as disclosed in its 2025 Annual Report. Formatted for executive readability.

At a Glance

COMPANY	FRAMEWORK	24/7 SOC	BOARD REPORTING	MATERIAL INCIDENTS	CERTIFICATIONS
Barclays PLC	**NIST CSF + ISO 27001**	**3 JOCs**	**Active**	**Phishing & Supply Chain**	**6**
LSE: BARC / NYSE: BCS	12-Standard policy	Global Joint Ops Centres	Board Risk Committee	Disclosed 2025	ISO 27001 (x4) + Cyber Essentials

Barclays PLC is a UK-headquartered global banking and financial services institution with $38.43 billion in annual revenue and approximately 93,000 employees worldwide. Its cybersecurity program is among the most formally structured in this peer group, featuring a dedicated Chief Information Security Office, 12 cybersecurity-specific policy standards, 24/7 Joint Operations Centres across three global locations, a Group CISO with 25+ years of experience, and multiple ISO 27001 certifications. In 2025, the Group disclosed experiencing cybersecurity incidents including phishing and supply chain attacks.

Key Context — Elevated Risk Profile: Barclays explicitly discloses that its cybersecurity risk profile is elevated, citing the onset of AI-enabled attacks, ongoing remediation work identified through cybersecurity testing, geopolitical threats, and evolving threat actor techniques. The Group also confirmed 2025 incidents involving phishing and supply chain compromise — a candid and important disclosure that reflects the reality facing even the most sophisticated programs.

1. Risk Management & Strategy

Barclays operates a comprehensive cybersecurity risk management program embedded within its Enterprise Risk Management Framework (ERMF). The program is built around an Information and Cyber Security Policy supported by 12 specific Standards and assessed against the NIST Cybersecurity Framework.

The 12 Cybersecurity Standards

• Cryptography	• Network Security
• Security Configuration	• Data Loss Prevention
• Vulnerability Management	• Data Security
• Incident Response & Threat Intelligence	• Threat Management
• Governance	• Identity & Access Management
• Third Party Information and Cyber Security	• Application Security

Elevated Risk Profile — 2025 Disclosure

AI-Enabled Attack Sophistication

Barclays explicitly flags the onset of AI as a risk amplifier — enabling more sophisticated social engineering, multi-step autonomous attacks via agentic AI systems, and expanded attack surface through AI-integrated tools.

Agentic AI Exposure

The Group's deployment of agentic AI with access to systems, data and third-party tools creates a novel attack surface. Threat actors may exploit permissioning controls to manipulate AI agents into executing unauthorised actions.

Geopolitical Threats

Geopolitical events could impact the Group directly or indirectly through its critical suppliers or national infrastructure — a risk heightened by the Group's global footprint and systemically important status.

Legacy Technology

Certain legacy technologies at or approaching end-of-life may not maintain acceptable security levels — a known risk factor across large financial institutions with decades of accumulated technology infrastructure.

Supply Chain Incidents (2025)

Third-party suppliers experienced successful cyber compromises in 2025, including ransomware attacks that disrupted operations and, in some cases, impacted Barclays' own operations.

2. Governance & Leadership

Role / Body	Cybersecurity Responsibilities	Notes
Group CISO	Heads the Chief Information Security Office. Responsible for all cybersecurity risk assessment and management. Approves and is accountable for the Information and Cyber Security Policy and all 12 associated Standards.	25+ years managing cybersecurity for global financial institutions. Advanced degrees. Reports to Group Co-COOs.
Business/Regional CISOs & BISOs	Team of CISOs and Business Information Security Officers supporting business units, regions and jurisdictions globally.	Accountable for day-to-day residual risk monitoring, gap identification, remedial action oversight, and strategy implementation.
Board Risk Committee	Primary Board-level oversight body for cybersecurity. Received CISO updates in 2025 on threat environment, ransomware preparedness, risk posture, incident trends, vulnerability management, and regulatory developments.	Oversees cybersecurity as part of Operational Risk principal risk category.
Group Co-COOs	CISO reports directly to Group Co-Chief Operating Officers. Provide updates to the full Board on cybersecurity capability strengthening and risk reduction progress.	Members of the Group Executive Committee.
Cybersecurity Risk Category Controls Forum	Receives input from 12 Cyber Control Standards Councils (one per Standard). Feeds into Group Controls Committee → Group Risk Committee → Board Risk Committee.	Multi-tier governance escalation chain ensuring Board visibility of all 12 cybersecurity domains.
Internal Audit & Operational Risk	Provide independent second and third line of defence perspectives on cyber risk management.	Ensures independent verification of cybersecurity controls and program effectiveness.

Governance Strength: Barclays operates one of the most formally structured cybersecurity governance frameworks in this peer group — with 12 dedicated Standards Councils feeding through a defined escalation chain to the Board Risk Committee, independent second and third line oversight from Internal Audit and Operational Risk, and direct CISO reporting to members of the Executive Committee. This level of structural formality is characteristic of globally systemically important banks.

3. Key Program Elements

Joint Operations Centres (JOCs)

Barclays operates 24/7 Joint Operations Centres from three globally strategic locations. The JOCs link security professionals and incident response managers with control functions and business unit representatives. During significant incidents, the Crisis Management Team monitors response and invokes Crisis Leadership Teams (CLTs) at entity, business unit, and regional levels.

Penetration Testing & Threat-Led Assurance

External security consultants conduct penetration tests, attack simulations, and independent capability reviews. In 2025, testing activities were undertaken as part of the CISO's threat-led assurance model. Barclays also partners with third-party providers for DDoS prevention, phishing simulations, vulnerability scanning, and industry benchmarking.

Third-Party Security Management

A dedicated Third Party Security Management team conducts risk-based assurance over suppliers and their partners against contractual Information and Cyber Security Supplier Control Obligations. Activity prioritises suppliers underpinning the most important business services. Barclays proactively alerts suppliers when vulnerability is anticipated.

Operational Resilience Framework

An established Operational Resilience Framework — integrated with the ERMF and embedded in the Barclays Controls Framework — governs recovery planning across cyber disruptions, technology failures, and colleague unavailability. Recovery plans are regularly tested with the aim of reducing the volume and impact of operational incidents year-on-year.

Data Privacy Program

A globally applicable Barclays Data Privacy Policy and associated Standards govern all data collection, use, and sharing. A Group Data Protection Officer (GDPO) reports privacy issues to the highest level of management. Annual data privacy training is mandatory for all colleagues. A dedicated team handles individual privacy requests through a publicly accessible mailbox.

Phishing Training & Simulation

A structured phishing simulation program provides education and awareness, with management interventions for susceptible employees. A one-click phishing report button is integrated into colleague email accounts, with feedback provided on whether reported emails were genuine threats. Metrics are used to continuously refine the program.

4. Certifications & Training

Certification	Description	Status
ISO 27001	Information Security Management System	**Certified (x4)**
Cyber Essentials	UK Government-backed cyber baseline certification	**Certified**
Cyber Essentials Plus	Enhanced version with independent technical verification	**Certified**
UK Digital Banking Certification	UK certification for digital banking security standards	**Certified**

Training Program Overview

Training Element	Status	Detail
Mandatory Annual Training	Yes — all permanent employees	Covers incident reporting, sensitive data protection, device security, data leakage, social engineering, and password management
Non-Completion Consequences	Yes — formal consequences	Non-completion may result in disciplinary action and impact to compensation — a notably strong enforcement mechanism
Phishing Simulations	Yes — operational program	Includes education, awareness exercises, and management interventions for employees who demonstrate susceptibility
One-Click Phish Reporting	Yes — email-integrated	Integrated tool enables colleagues to report suspicious emails to JOCs; feedback provided on whether email was genuine or suspect
Data Privacy Training	Yes — annual mandatory	Separate annual data privacy training reviewed and refreshed each year; additional tailored training provided as needed
Hybrid Working Security	Yes — ongoing education	Continued education on cybersecurity risks specific to remote/hybrid working environments including data exploitation and leakage risks

5. Program At-a-Glance Scorecard

Group CISO (25+ years experience)	Confirmed	24/7 Joint Operations Centres (x3 global)	Confirmed
NIST CSF Framework Adopted	Confirmed	12 Cybersecurity Policy Standards	Confirmed
ISO 27001 Certification (x4)	Certified	Cyber Essentials / Essentials Plus	Certified
UK Digital Banking Certification	Certified	Board Risk Committee Oversight	Active
Multi-Tier Governance Escalation Chain	Confirmed	Internal Audit (3rd Line) Review	Confirmed
Penetration Testing Program	Confirmed	Threat-Led Assurance Model (2025)	Confirmed
Third-Party Security Mgmt Team	Confirmed	Contractual Supplier Security Obligations	Confirmed
Operational Resilience Framework	Confirmed	Crisis Leadership Teams (CLTs)	Confirmed
Mandatory Annual Training — All Staff	Annual	Phishing Simulations + Interventions	Confirmed
One-Click Phish Reporting Tool	Confirmed	Annual Data Privacy Training	Annual
Group Data Protection Officer (GDPO)	Confirmed	Cyber Insurance Coverage	Confirmed
Elevated Cybersecurity Risk Profile	Elevated	2025 Incidents (Phishing/Supply Chain)	Disclosed

6. Key Observations & Benchmarking Notes

Best-in-Class Governance Structure

Barclays' multi-tier governance model — 12 Standards Councils → Controls Forum → Group Controls Committee → Group Risk Committee → Board Risk Committee — is among the most formally structured of any peer group company reviewed. Combined with independent second and third line oversight from Operational Risk and Internal Audit, this represents a genuinely sophisticated governance architecture.

Six Active Security Certifications

Four ISO 27001 certifications plus Cyber Essentials, Cyber Essentials Plus, and UK Digital Banking certification — six in total — is the highest certification count observed in the peer group and reflects a commitment to independently validated security standards.

Industry-Leading Training Enforcement

Consequences for non-completion of mandatory training — including disciplinary action and compensation impact — is a notably strong enforcement mechanism. Most companies describe mandatory training without specifying consequences for non-compliance. Barclays' approach signals genuine cultural accountability.

Candid Elevated Risk Disclosure

Barclays is one of few companies in the peer group to explicitly state that its cybersecurity risk profile is 'elevated' — citing AI, geopolitical threats, and ongoing remediation work. This level of transparency is commendable and more informative to stakeholders than generic boilerplate risk language.

2025 Supply Chain Incidents Confirmed

Barclays disclosed that third-party suppliers experienced cybersecurity compromises in 2025, including ransomware attacks that in some cases impacted Barclays' own operations. While not a material Barclays system breach, this is a more specific incident disclosure than most peers provide and highlights the ongoing supply chain threat to large financial institutions.

Agentic AI Risk — Forward-Looking Disclosure

Barclays is one of very few companies to explicitly address agentic AI as a cybersecurity risk factor — noting that AI agents with system access create an expanded attack surface for multi-step autonomous attacks. This forward-looking disclosure reflects sophisticated threat awareness beyond standard AI risk language.

Source: Barclays PLC Annual Report 2025. Cybersecurity disclosures extracted from the Risk Management section. Original document available at: https://home.barclays/investor-relations/results-and-reports/annual-reports/ | Prepared: May 07, 2026 | For Internal Distribution Only