CONSUMER DUTY ALLIANCE

CYBERSECURITY OVERVIEW & CHECKLIST 2026

Digital threats to your business

A key focus of the Consumer Duty's cross-cutting rules is to avoid foreseeable harm to retail customers and in today's environment, cyber risk is one of the most impactful, potential foreseeable harms facing financial advice firms, their staff and their clients. Financial professionals are entrusted with protecting consumer interests, safeguarding sensitive information, and maintaining the trust that underpins every client relationship.

Navigating digital security is central to that responsibility.

Cyber threats are escalating rapidly. According to recent research, nearly half of all UK businesses experienced a cyber breach or attack in the past 12 months, rising to 67% among medium-sized firms. Financial services remains one of the most targeted sectors, with attackers motivated by the large volumes of valuable financial client data they can access. The scale of the threat is growing too — more than 560,000 new cyber threats are discovered every day, and 81% of UK businesses hit by cyber attacks are SMEs.

The rapid evolution of AI has further amplified both the speed and sophistication of attacks, making traditional defences less effective and increasing the likelihood of harm if firms do not adapt.

This practical cyber security overview has been created to help you identify where your defences may need strengthening and to support you in meeting the expectations of the ICO, FCA and other regulatory bodies. Our aim is simple: to help you protect your clients, your firm, and the trust that sits at the heart of your service.

With thanks to the team at Mailock.com for their support with this guide.

Keith Richards
CEO, Consumer Duty Alliance

TOP 10 CYBERSECURITY THREATS TO YOUR ORGANISATION

Malware
A broad term for malicious software designed to harm, exploit, or take control of devices, networks, or systems.

Key action: Protect endpoint devices such as laptops, desktops, and mobile phones with reliable antivirus software and regular updates.

Man-in-the-Middle
When attackers intercept and manipulate communications between two parties without their knowledge.

Key action: Secure communication channels, such as emails, messaging apps, and internal systems, with encryption and authentication in line with ICO/FCA requirements.

Phishing
When attackers deceive individuals into revealing sensitive information by pretending to be trustworthy entities in communications.

Key action: Train employees across all departments, particularly customer service and finance teams, to recognise and avoid suspicious emails or communications.

Supply Chain Attack
A tactic where attackers compromise an organisation by infiltrating less secure elements of its supply chain.

Key action: Closely monitor third-party vendors and suppliers to ensure they adhere to your security standards.

Distributed Denial of Service (DDoS)
An attack that overwhelms a network, server, or website with excessive traffic, causing disruptions or outages.

Key action: Safeguard IT infrastructure, including web servers and online platforms, with scalable bandwidth and robust firewalls.

SQL Injection
When attackers insert malicious SQL code into a database query, allowing them to access or manipulate data without authorisation.

Key action: Safeguard databases and web applications, particularly client portals and sales systems, with input validation and web application firewalls.

Brute Force
A method of attack where automated systems attempt every possible combination of passwords or keys to gain access to a system.

Key action: Enforce strong password policies and two-factor authentication across all business systems

Human Error
Mistakes made by employees, such as clicking on phishing links or sending sensitive information to the wrong person, which can lead to a data breach.

Key action: Implement organisation-wide cybersecurity awareness and assessment programmes and clear incident reporting procedures for all employees.

Credential Stuffing
An attack where cybercriminals use stolen username and password combinations from one breach to gain unauthorised access to other systems.

Key action: Protect user accounts on HR, finance, and customer-facing systems with password monitoring tools and regular security audits.

Zero-Day Exploit
An attack that targets previously unknown vulnerabilities in software or hardware, exploiting them before developers can issue a patch.

Key action: Ensure all software and hardware systems, including legacy platforms, are updated promptly with the latest security patches and updates.

CYBERSECURITY CHECKLIST

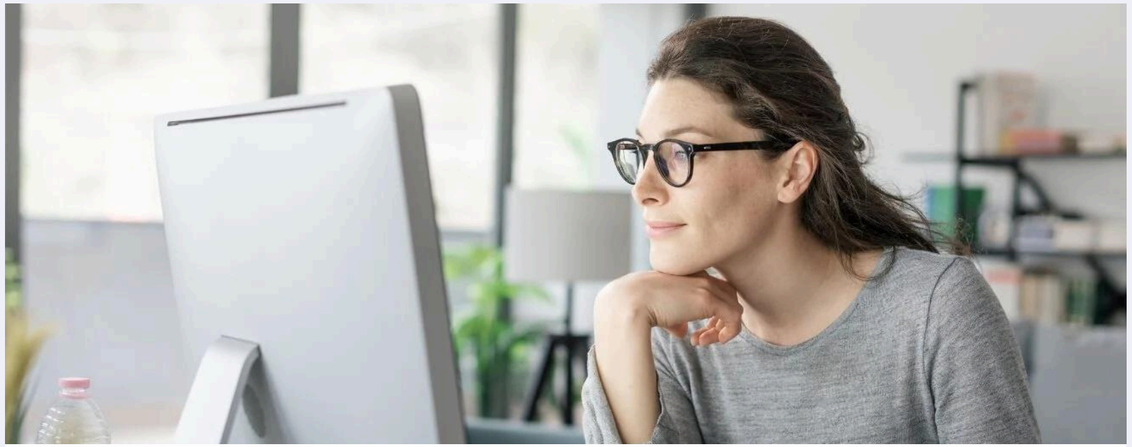
To fill out this cybersecurity checklist, review your current security measures and note your existing solutions or requirements for each attack vector in the "Your Solution or Need" column.

Name & Title : _____ Date_____

Cybersecurity Threat	Example Mitigation	Your Solution or Need
Malware	Install anti-malware software	
Phishing	Regular staff training and test phishing emails	
DDoS	Robust firewall and scalable bandwidth	
Brute Force	Ensure 2-factor or multi-factor access controls are in place on all critical systems	
Credential Stuffing	Use password management tools, audit with password monitoring tools	

Cybersecurity Threat	Example Mitigation	Your Solution or Need
Man-in-the-Middle	Secure outbound email with encryption & provide clients with a secure reply pathway (example: Mailock)	
Supply Chain Attack	Document and share a security standard that you expect your suppliers to adhere to	
SQL Injection	Implement input validation and establish a web application firewall	
Human Error	Regular cybersecurity training for all staff and an incident reporting process	
Zero Day Exploit	Establish a process for installing all system updates promptly	

Additional Resources



FREE REPORT DOWNLOAD

Get the full 2026 cybersecurity paper

Understand the key cyber threats in detail

Get a comprehensive overview of the latest cybersecurity threats and best practices to safeguard businesses in 2026.

Download paper