Cybersecurity Paper 2026

An overview of the latest cybersecurity threats and good practices to safeguard financial service businesses in 2026.

CONSUMER DUTY ALLIANCE

Contents

With thanks to Mailock.com for the production of this paper

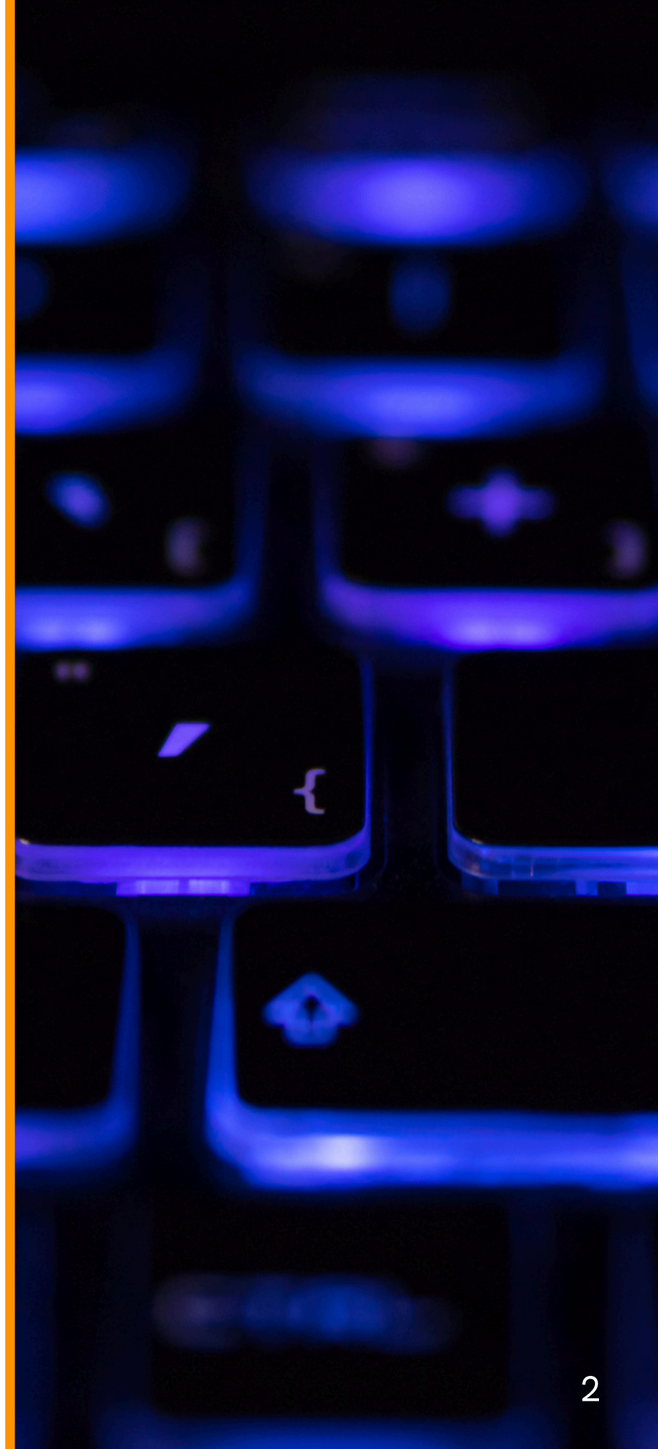
What Is Cybersecurity?

Cybersecurity refers to the practice of safeguarding systems, networks, and programmes from digital attacks. These attacks typically aim to access, modify, or destroy sensitive information, extort money from users, or disrupt normal business operations. However, the rapid evolution of artificial intelligence (AI) has dramatically amplified both the speed and sophistication of these threats. AI not only accelerates the cadence of attacks but also enhances their precision, making traditional defense measures increasingly vulnerable. As outlined in this paper, the integration of AI into the threat landscape represents a profound and escalating risk to cybersecurity at every level.

At its core, cybersecurity involves implementing a range of technologies, processes, and practices designed to protect digital assets from threats. As the volume of data increases, more devices become interconnected, and the evolution of AI becomes more prevalent, cybersecurity becomes increasingly vital for both individuals and organisations.

Key areas of cybersecurity include:

- Network security: Protecting the integrity and usability of network infrastructure.
- Information security: Securing sensitive data from unauthorised access.
- Application security: Ensuring that applications are protected from threats.
- Operational security: Managing and safeguarding how data is handled and protected.
- Cloud security: Protecting data in cloud environments from unauthorised access.
- Endpoint security: Securing individual devices, such as laptops and mobile phones.
- Physical security: Safeguarding physical infrastructure, such as servers and data centres.



Key Definitions

The most used industry terms (and their definitions) that you need to be aware of include:

- Attack surface: The total sum of the vulnerabilities and entry points in a system or network that could be exploited by an attacker. Reducing the attack surface is a core goal of cybersecurity efforts.

- Threat actor: An entity that is responsible for an event that impacts, or has the potential to impact, the security of an organisation's network, systems, or data. This could include hackers or insider threats.

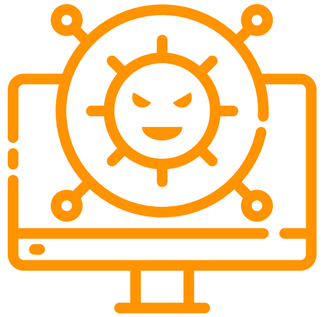
- Insider threat: A security risk that originates from within the targeted organisation. It could be an employee, contractor, or business partner who has access to critical information or systems and misuses that access, whether maliciously or unintentionally.

- Human error: An unintentional action by an individual that compromises the security of systems, networks, or data. Examples include misconfiguring systems, using weak passwords, or falling victim to phishing attacks. Human error is a common factor in cybersecurity breaches and can create exploitable vulnerabilities.

- Vulnerability: A weakness or flaw in a system, network, or application that can be exploited by a threat actor to gain unauthorised access or cause damage. Identifying and patching vulnerabilities is crucial for maintaining security.

Common Types Of Attacks

Cyberattacks come in various forms, each designed to exploit vulnerabilities in systems and networks, leading to potential data breaches, disruptions, or financial losses. Artificial Intelligence (AI) is increasing the risk further. Here are the top types to be aware of:

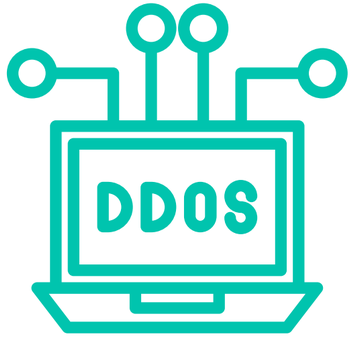


Malware

A broad term for any type of malicious software designed to harm, exploit, or take control of devices, networks, or systems. Common types of malware include viruses, worms, ransomware, and spyware.

Phishing

A form of social engineering attack where attackers deceive individuals into revealing sensitive information, such as passwords and credit card numbers, by pretending to be trustworthy entities in communications.



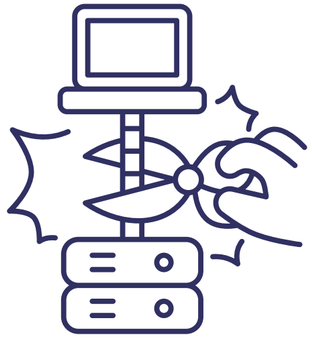
DDoS

Distributed Denial-of-Service attacks are when multiple compromised systems are used to flood a targeted server or network with traffic, overwhelming it and causing service disruptions or outages.

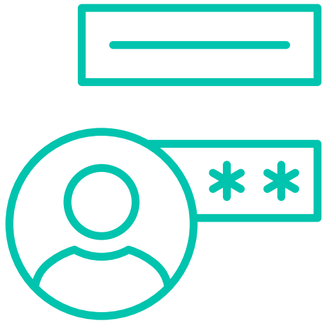
Brute Force

A trial-and-error method to systematically guess passwords by trying possible combinations until the correct one is found. This process can be automated, allowing attackers to test a large number of credentials.

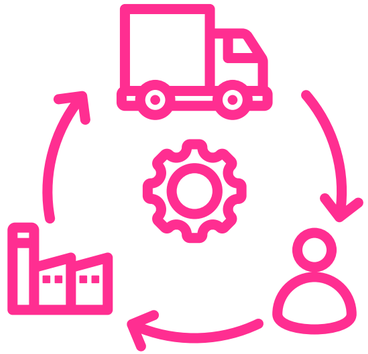
Common Types Of Attacks (cont.)



Man-in-the-Middle
A type of attack where the attacker secretly intercepts communication between two parties. The threat actor can eavesdrop, alter, or steal sensitive information being exchanged.



Credential Stuffing
A type of cyberattack where attackers use lists of compromised usernames and passwords from previous data breaches to gain unauthorised access to user accounts through automated login attempts.



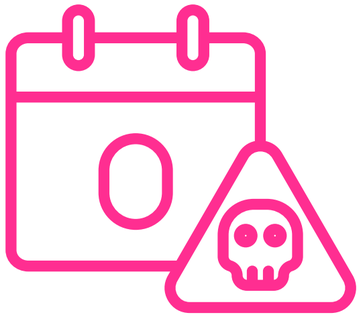
Supply Chain Attack
When cybercriminals target vulnerabilities in a company's supply chain or third-party providers. By compromising these vendors, attackers can infiltrate an organisation or its customers.

SQL Injection
A web-based attack where an attacker inserts malicious SQL code into a query input field in order to manipulate the underlying database. This can lead to data theft, unauthorised access, or database corruption.

Common Types Of Attacks (cont.)

Human Error

Employee errors like falling for phishing attempts or mistakenly sharing confidential data with unintended recipients can result in unauthorised access and potential data breaches.



Zero-Day Exploit

A cyberattack that exploits undiscovered flaws in software or hardware, taking advantage of the gap before a fix or security update is released.

The Rise of Artificial Intelligence

Artificial intelligence has significantly transformed the cyber threat landscape, both enhancing security measures and simultaneously introducing new avenues for cyberattacks. On one hand, AI-powered tools have revolutionised threat detection and response, enabling firms to identify patterns of malicious activity in real-time and automate defenses more efficiently than ever before. Machine learning algorithms can now analyse massive volumes of data to predict and pre-empt potential breaches, reducing the time it takes to detect threats from months to mere minutes. This proactive defence approach marks a major advancement from traditional reactive cybersecurity methods.

However, the same capabilities that bolster defences are being leveraged by threat actors to develop more sophisticated attacks. Cybercriminals are using AI to craft convincing phishing emails, mimic human behaviour in social engineering schemes, and even automate the discovery of system vulnerabilities. Deepfakes, powered by generative AI, have emerged as a tool for fraud and misinformation, complicating efforts to verify the authenticity of digital content. As AI continues to evolve, the cyber threat landscape is becoming more dynamic, creating a high-stakes arms race between attackers and defenders.

AI Driven Cyber Threat Matrix

Attack Type	How AI amplifies	Risk for firms	Risk levels
Malware	Creates polymorphic, self-mutating malware that evades detection	Basic antivirus can't catch evolving threats	High
Phishing	Crafts hyper-personalised, convincing phishing emails using public data	Employees are less trained and more susceptible	High
Distributed Denial-of-Service (DDoS)	Orchestrates massive botnet attacks with better timing and targeting	Few small firms have DDoS protection or back up systems in place	High
Brute Force	Uses intelligent password guessing, speeding up attempts	Weak passwords make for easier targets	High
Man-in-the-Middle	Identifies unsecure communications and intercepts data in real time	Lack of encryption/VPN use increases risk	High
Credential Stuffing	Automates login attempts across platforms using stolen data	Password reuse is common; Multi-Factor Authentication (MFA) often missing	High
Supply Chain Attack	Maps out weak vendors to use them as attack pathways	Small firms may become an easy entry point into larger ecosystems	High
SQL Injection	Automates vulnerability scanning of databases and web apps	Poorly secured websites or customer portals are easy to exploit	Medium-High

Impact Of A Data Breach

According to GOV.uk, half of businesses (50%) and around a third of charities (32%) have experienced some form of cybersecurity breach or attack in the last 12 months. But what are the impacts of this on your business?

1

Financial Impact

The financial consequences of a data breach can be devastating for firms:

- Immediate response costs: Firms may need to pay upfront costs for forensic investigations, containment, and engaging with cybersecurity consultants.
- Regulatory fines: The Information Commissioner's Office (ICO) plays a key role in enforcing data protection laws and can fine firms up to £17.5 million or 4% of their global turnover, whichever is higher, depending on the severity of the breach.
- Ransom payments: While the UK government discourages paying ransoms, some firms, particularly SMEs, may feel compelled to do so to recover data or avoid public exposure.
- Revenue loss: Downtime from a data breach can be particularly damaging for firms, leading to a loss in revenue from disrupted operations.

Impact Of A Data Breach (cont.)

2

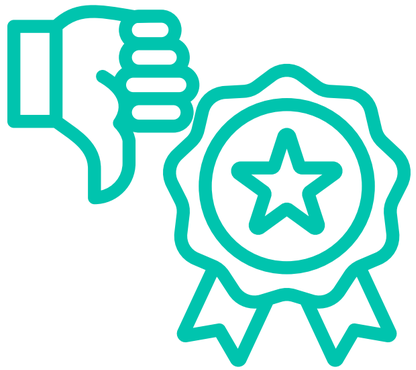
Reputational Damage

The damage from a data breach can have long-term effects on the reputation of your firm. UK consumers are becoming increasingly aware of data privacy and protection. A breach can result in significant loss of trust, particularly if personal or financial data is exposed. According to research, 41% of UK consumers would stop doing business with a company following a serious data breach.

3

Operational Disruptions

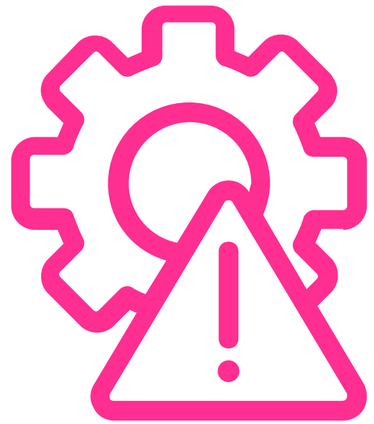
The operational impact of a data breach can be substantial. Many UK businesses, from financial services to online retailers, depend on uninterrupted digital operations. A cyber-attack or breach can disrupt services, resulting in lost data and missed business opportunities. In some cases, critical infrastructure, such as the UK's National Health Service (NHS), has been targeted, leading to severe operational disruption.



4

Loss of Software, Hardware, and Data

The impact of a data breach extends beyond the exposure of sensitive information; it can result in the loss or damage of critical infrastructure, with firms facing devastating setbacks when compromised. Ransomware attacks, for instance, often disable key systems, requiring firms to either pay to regain access or rebuild from scratch. In many cases, valuable data can be permanently lost or corrupted.



Cybersecurity And Regulation

Businesses in regulated sectors must adhere to various regulatory standards to ensure cybersecurity practices are sufficient.

Data Protection Act 2018 & UK GDPR	Explicitly mandates the implementation of "appropriate technical and organisational measures" to protect personal data (Article 32). This includes ensuring data confidentiality, integrity, and availability through encryption, secure access controls, and risk assessments.
FSMA 2000 & FCA Regulations	Under FSMA, financial institutions must adhere to the FCA's operational resilience requirements. The FCA mandates that firms have "effective systems and controls" in place to prevent data breaches and financial crime (SYSC 3.2.6R). This is reinforced by the FCA's announcement (PS25/13) on email being classified as a durable medium.
Network & Information Systems 2018	Applies to operators of essential services such as those in healthcare, transport, energy, and digital infrastructure. These businesses must implement appropriate security measures to manage risks posed to network and information systems (Regulation 10).
Payment Services Regulations & PSD2	Requires payment service providers to ensure the security of customer data and financial transactions (Article 95). This includes strong customer authentication, typically multi-factor authentication, to verify users' identities, alongside encryption to protect payment data.
MiFID II (Markets in Financial Instruments Directive)	Financial institutions must implement effective risk management systems, including measures to secure IT infrastructure (Article 16). This includes ensuring the confidentiality and integrity of data, preventing cyberattacks, and having robust business continuity plans.

In Focus: Consumer Duty

The FCA’s Consumer Duty, described in PS22/9 and FG22/5, requires financial services firms to deliver outcomes that protect consumer interests.

While the Duty focuses on improving consumer care, it also demands robust data protection and cybersecurity measures to ensure the security of customer information, which directly supports the obligation to prevent foreseeable harm.

Firms are expected to:

- Ensure that their systems are secure to avoid data breaches, aligning with the Consumer Duty’s expectation of firms taking "all reasonable steps" to avoid harm to customers.
- Use secure methods (e.g. multi-factor authentication to access encrypted emails or client portals) to prevent unauthorised access to customer data, supporting the Duty’s objective to "minimise harm" and secure customer information.

Network Security

What is it?

Network security involves protecting the integrity, confidentiality, and availability of an organisation’s internal and external networks. It prevents unauthorised access, misuse, or attacks on the network infrastructure, ensuring smooth communication and safe data exchanges.

Good practices

- Penetration testing and external audits: Regularly test your systems to find security weaknesses and fix them. Use external audits, like Cyber Essentials certification, to ensure compliance with security standards and strengthen defences against emerging threats.
- Firewalls: Use firewalls to watch and control the data coming in and out of your network. They help make sure only approved connections are allowed.
- Intrusion Detection and Prevention Systems (IDPS): These tools help spot suspicious or harmful activity on your network, and can block it automatically to keep your systems safe.
- Network segmentation: Break your network into contained sections so that only the right people or systems can access each part. This helps contain any security issues and prevents them from spreading.

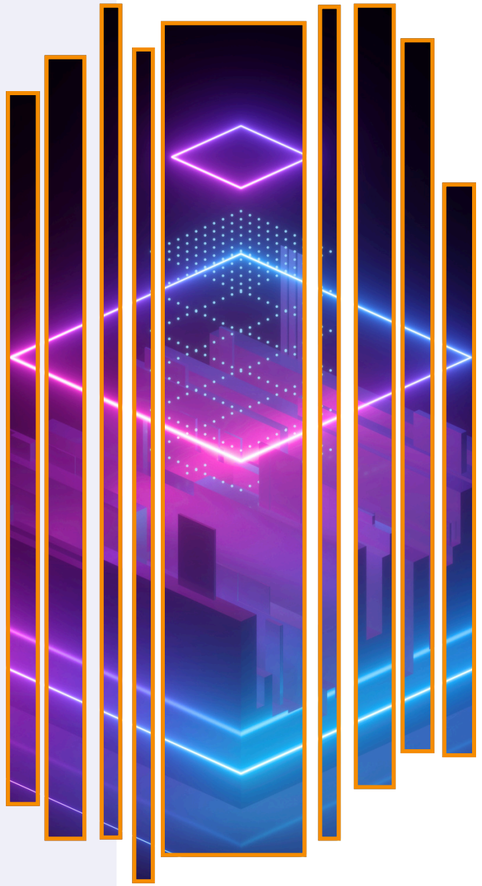
Information Security

What is it?

Information security (InfoSec) is the practice of protecting information by mitigating security risks related to unauthorised access, misuse, or modification. It ensures the confidentiality, integrity, and availability of data, whether it is stored or being transmitted. InfoSec plays a critical role in safeguarding sensitive information and maintaining compliance with regulations such as GDPR.

Good practices

- Data encryption: Encrypt sensitive data, both at rest and in transit, to ensure that it remains protected from unauthorised access. Email encryption tools can secure communications and prevent data interception.
- Access control: Implement role-based access controls to restrict who can access certain data, ensuring only authorised personnel can view or modify sensitive information.
- Multi-Factor Authentication (MFA): Provides an extra layer of security, ensuring that users must authenticate with two or more methods (e.g., a password and a verification code) to access sensitive systems such as portals or data.
- Staff training and regular audits: Perform routine security audits to identify vulnerabilities and ensure compliance with data protection standards, as well as providing regular Cybersecurity and GDPR training and assessment for employees to raise awareness and reduce human error.



Application Security

What is it?

Application security protects software applications from internal and external threats. Given the rise of web-based applications, ensuring these systems are secure is crucial for preventing exploits like SQL injection or cross-site scripting (XSS).

Good practices

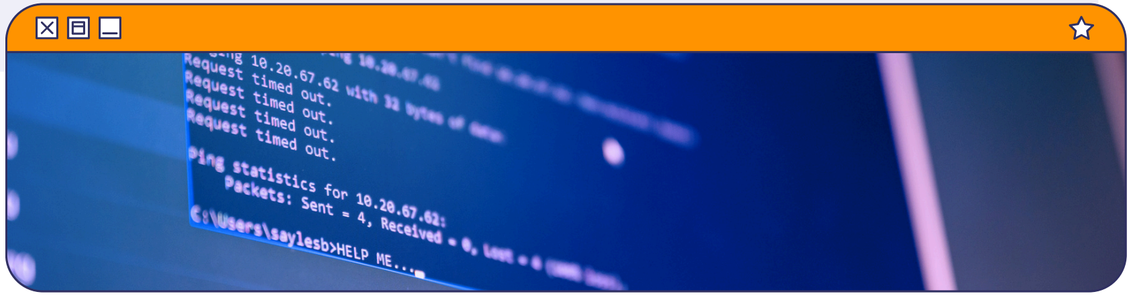
- Secure development lifecycle: Integrate security into every stage of the development process, from design to deployment, with regular code reviews and security testing.
- Patch management: Ensure all applications are regularly updated and patched to fix vulnerabilities that could be exploited by attackers.
- Web Application Firewalls (WAFs): Deploy WAFs to filter and block malicious web traffic targeting your applications.
- MFA for application access: Implement MFA for accessing critical applications to reduce the risk of unauthorised access, especially for systems containing sensitive or personal information.

Operational Security

What is it?
Operational security focuses on securing the processes and systems used within the firm to handle sensitive data and resources. It involves ensuring that information is protected throughout its lifecycle, from creation to disposal.

Good practices

- Comprehensive security policies: Establish security policies for the handling and access of sensitive data. Develop robust business continuity plans to ensure the firm can continue to operate in the event of a cyber incident.
- Vendor management: When selecting third-party vendors, ensure they adhere to strong security protocols. Look for certifications such as ISO 27001, Cyber Essentials, or SOC (Service Organisation Control) reports, which demonstrate compliance with industry standards. Additionally, consider the data storage location: ensure the country where data is stored has data adequacy agreements in place to meet international compliance, such as with GDPR.
- Risk assessments: Conduct regular risk assessments to identify vulnerabilities in your operational processes and take the necessary steps to mitigate them.
- Access controls: Implement access controls to ensure that only authorised individuals can reach sensitive systems, reducing the risk of unauthorised access and data breaches.



Cloud Security

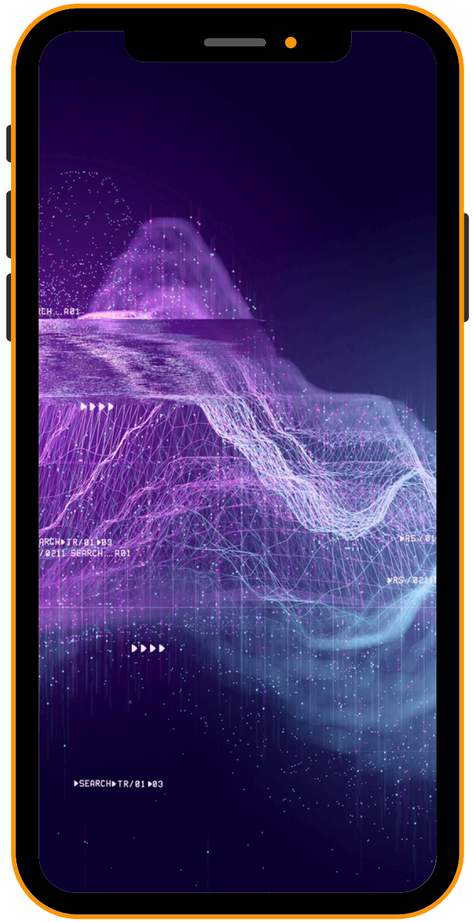
What is it?

Cloud security focuses on protecting data, applications, and services hosted in cloud environments. It addresses unique challenges such as misconfigurations and exposed APIs (Application Programming Interface). In cloud security, both the cloud provider and the firm have distinct roles: the provider is responsible for securing the infrastructure, while the firm must secure data, access, and applications within the cloud.

Good practices

- Identity and access management (IAM): Control access to cloud resources, ensuring only authorised personnel can interact with sensitive systems and data.
- Configuration audits: Regularly audit cloud configurations to detect and rectify misconfigurations that could leave the environment vulnerable.
- Data encryption: Ensure that data stored and transmitted in the cloud is encrypted, providing an extra layer of protection against unauthorised access.
- Backup and disaster recovery: Utilise secure cloud backups and develop a disaster recovery plan to maintain business continuity in the event of an incident.

Endpoint Security



What is it?

Endpoint security protects devices such as laptops, desktops, mobile phones, and tablets that connect to a firm’s network. Each endpoint represents a potential entry point for attackers, making their protection critical to overall cybersecurity.

This includes not only company-issued devices but also personal devices used for work purposes under Bring Your Own Device (BYOD) policies. When staff use their own mobiles or tablets to access work emails, systems, or data, those devices must also be secured to prevent unauthorised access, data leakage, or malware infections.

Good practices

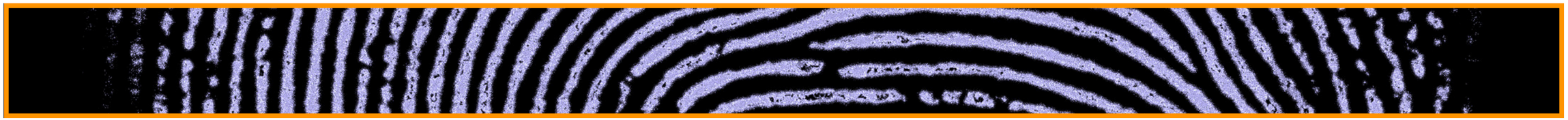
- Anti-virus and anti-malware software: Ensure all devices have updated anti-virus and anti-malware protection to detect and neutralise threats targeting endpoints.
- Endpoint Detection and Response (EDR): Implement EDR solutions that continuously monitor endpoint activities, detect threats, and respond in real-time.
- Mobile Device Management (MDM): Use MDM solutions to secure mobile devices, allowing for remote wiping or locking if a device is lost or stolen.
- Encryption for device storage: Encrypt data stored on endpoint devices, especially mobile and remote devices, to protect against data theft if devices are compromised.

Physical Security

What is it?
Physical security focuses on protecting hardware, servers, data centres, and other critical infrastructure from physical threats such as theft, natural disasters, or unauthorised access.

Good practices

- Controlled access: Use biometric scanners, keycards, or security guards to control physical access to sensitive areas, such as server rooms and data centres.
- Surveillance systems: Implement cameras and monitoring systems to deter and detect unauthorised access or suspicious activity in real-time.
- Environmental controls: Protect physical infrastructure from environmental hazards by installing fire suppression systems, temperature controls, and uninterruptible power supplies (UPS).
- Secure hardware disposal: Ensure all outdated or damaged hardware is securely wiped or physically destroyed to prevent data recovery from discarded devices.



Email Compliance For Regulated Businesses

Following clarification from the Financial Conduct Authority (FCA) that email can constitute a durable medium (PS25/13) where it enables information to be stored, accessed, and reproduced unchanged for an adequate period, firms must ensure their email communications meet specific security, integrity, and record-keeping standards.

Your obligations	What the regulations say	Are you compliant?
Encrypt Encrypt emails containing personal data	"Have a policy governing encrypted email, including guidelines that enable staff to understand when they should or should not use it. For example, there may be a guideline stating that any email containing sensitive personal data (either in the body or as an unencrypted attachment) should be sent encrypted." [ICO - GDPR]	
Audit Keep auditable copies of outbound emails	"Keep a copy of relevant electronic communications, made with, sent from or received on equipment: (1) provided by the firm to an employee or contractor; or (2) the use of which by an employee or contractor has been sanctioned or permitted by the firm." [FCA - COBS]	
Authenticate Authenticate recipients to prevent unauthorised access	“Have sound security mechanisms in place to guarantee the security and authentication of the means of transfer of information, minimise the risk of data corruption and unauthorised access and to prevent information leakage maintaining the confidentiality of the data at all times.” [ESMA - MIFID I]	
Revoke Have the capability to revoke misfired emails	"[in the event of a data breach] act quickly. Try to recall the email as soon as possible. If you can’t recall it, contact the person who received it and ask them to delete it." [ICO - GDPR]	
Reply Provide customers a secure way to communicate with you	"Ensure consumers receive communications they can understand, products and services meet their needs and offer fair value, and the support they need. Secure two-way communication channels support Consumer Duty and durable communication standards.” [FCA - Consumer Duty]	

More information about the creators of this paper

Consumer Duty Alliance

The Consumer Duty Alliance (CDA) is an independent professional body that is dedicated to helping advice firms turn regulation into meaningful, workable practice and raise standards together. Through the Alliance and its cross-sector working groups — including the Consumer Duty Data Forum —members gain practical support, a stronger collective voice, and access to a professional community that genuinely puts clients first.

The CDA works closely with policymakers and the regulator to ensure the value of professional advice is recognised and protected and that they understand the challenges of smaller firms in particular. As a not-for-profit, built by the sector, for the sector its purpose is to support advisers, firms and their clients without commercial influence.

Mailock

Mailock is a secure email solution designed to safeguard sensitive communications through end-to-end encryption and multi-factor authentication. It enables organisations to send confidential information securely while supporting compliance with regulatory requirements such as GDPR and Consumer Duty.

Following clarification from the Financial Conduct Authority (FCA) that email can meet the definition of a “durable medium” where certain conditions are satisfied, secure email solutions such as Mailock have become even more significant. By ensuring communications are encrypted, tamper-evident, securely delivered, and accessible for future reference, Mailock helps organisations meet both regulatory expectations and durable medium requirements.

By encrypting emails and verifying recipients before access is granted, Mailock provides assurance that sensitive customer data remains protected from cyber threats and unauthorised disclosure. Beyond strengthening security and compliance, it also helps reduce reliance on physical mail, lowering operational costs and supporting sustainability objectives.