Department for
Digital, Culture,
Media & Sport

UK Cyber Security Policy: Cyber Resilience

Naomi Gilbert, Head of Cyber Resilience Policy

17 November 2022

UK National Cyber Strategy

Strengthening the cyber ecosystem

Pillar 1

Strengthening the UK cyber ecosystem

Building cyber resilience

Pillar 2

Building a resilient and prosperous digital UK

Future technology

Pillar 3

Taking the lead in the technologies vital to cyber power

International

Pillar 4

Advancing UK global leadership and influence

Countering cyber threat

Pillar 5

Detecting, disrupting and deterring adversaries

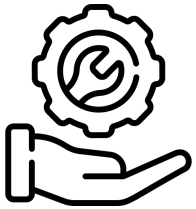
National Cyber Security Centre

Cyber Resilience: The challenges

Attacks: Nearly four in ten (39%) UK businesses and three in ten (30%) charities identified a cyber breach or attack in the past 12 months. Larger organisations were more targeted. Yet only just over half (54%) of businesses have taken action to identify cyber risks.

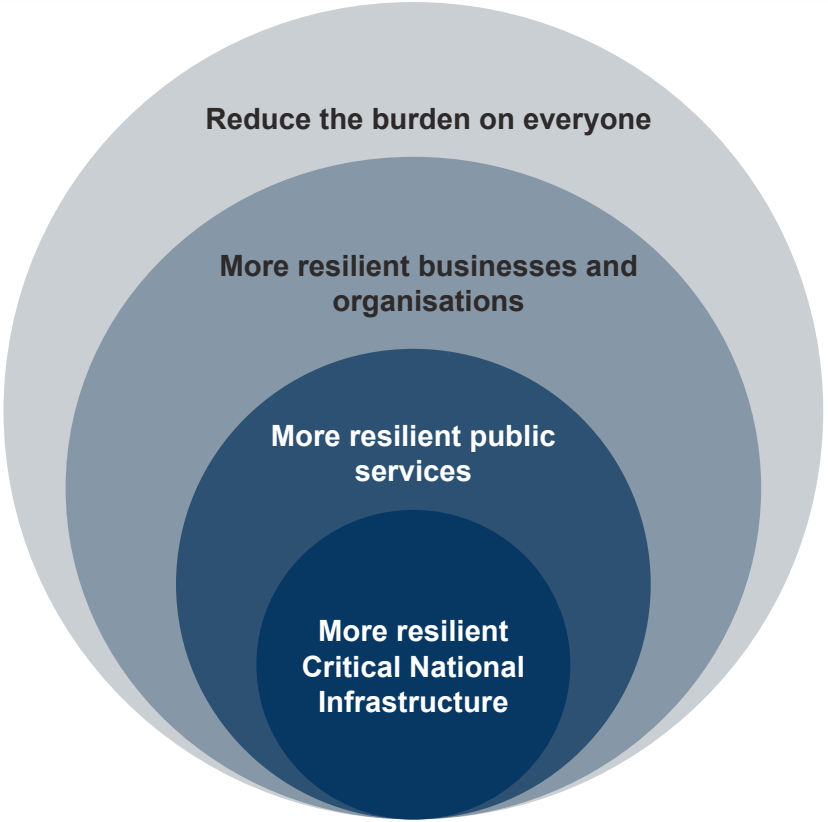
Senior leadership and boards:

- 82% of boards see cyber security as a ‘very high’ or ‘fairly high’ priority
- But there is a lack of engagement, understanding and action at senior leadership level.



Organisations often still **see cyber security as a technical issue** and as a cost rather than an issue of operational resilience and digital business continuity.

Cyber Resilience: The approach



Technology security: Reducing the burden on individuals

Reducing the burden on individuals & organisations

- Focus on technology that underpins our lives **at scale**
- Centrality of **international collaboration**
- **Partnership** (public-private) approaches are critical

Consumer smart devices

- Code of Practice published 2018
- ETSI Standard EN 303 645 published 2020
- Legislation passed 2022

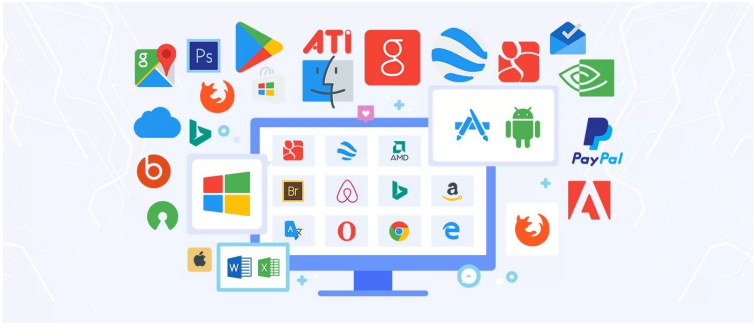
App stores

- Voluntary Code of Practice for App Stores Operators and App Developers for baseline security & privacy requirements

Technology security: Reducing the burden on organisations

Digital Service Providers

- Cloud providers, Online marketplaces & Search engines regulated under 2018 NIS Regulations
- Managed Service Providers proposed for future legislation



Software

- Enterprise software development, vendors, and use poses systemic risks
- High profile cyber attacks are increasingly facilitated by software vulnerabilities - Kaseya, SolarWinds

Cyber Resilience: The solutions

Foundations → **Incentives** → **Accountability** → **Regulations**

CYBER AWARE

National Cyber Security Centre

10 Steps to Cyber Security

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

Communicating costs

Market influencers

Holding accountable:

- Senior leaders
- Largest companies
- Organisations most critical to national security