FOXTECH

New UK Cyber Codes of Practice

What they are, and what that means for you

Presentation Agenda

1 Overview of the DSIT Codes of Practice and Their Relevance

2 Cyber Governance Code of Practice

3 Software Security Code of Practice

Introduction

About FoxTech

Effortless Cybersecurity. Built for Regulated Businesses

Security monitoring, vulnerability management, penetration testing and consultancy.

Iain Gibbons

CEO

Anthony Green

CTO

Matthew Wylie

Security and Infrastructure Engineer

Overview of the DSIT Codes of Practice and Their Relevance

Introduction to DSIT codes of practice

Codes of Practice

DSIT has developed voluntary Codes of Practice to set clear expectations for cyber security.

Why

"To address cyber risks not being sufficiently addressed by industry."

i.e. The UK Government expects UK businesses to do more in these areas.

Who are they for?

Codes of Practice

- Cyber Governance:

  Medium/Large orgs and small Tech Companies

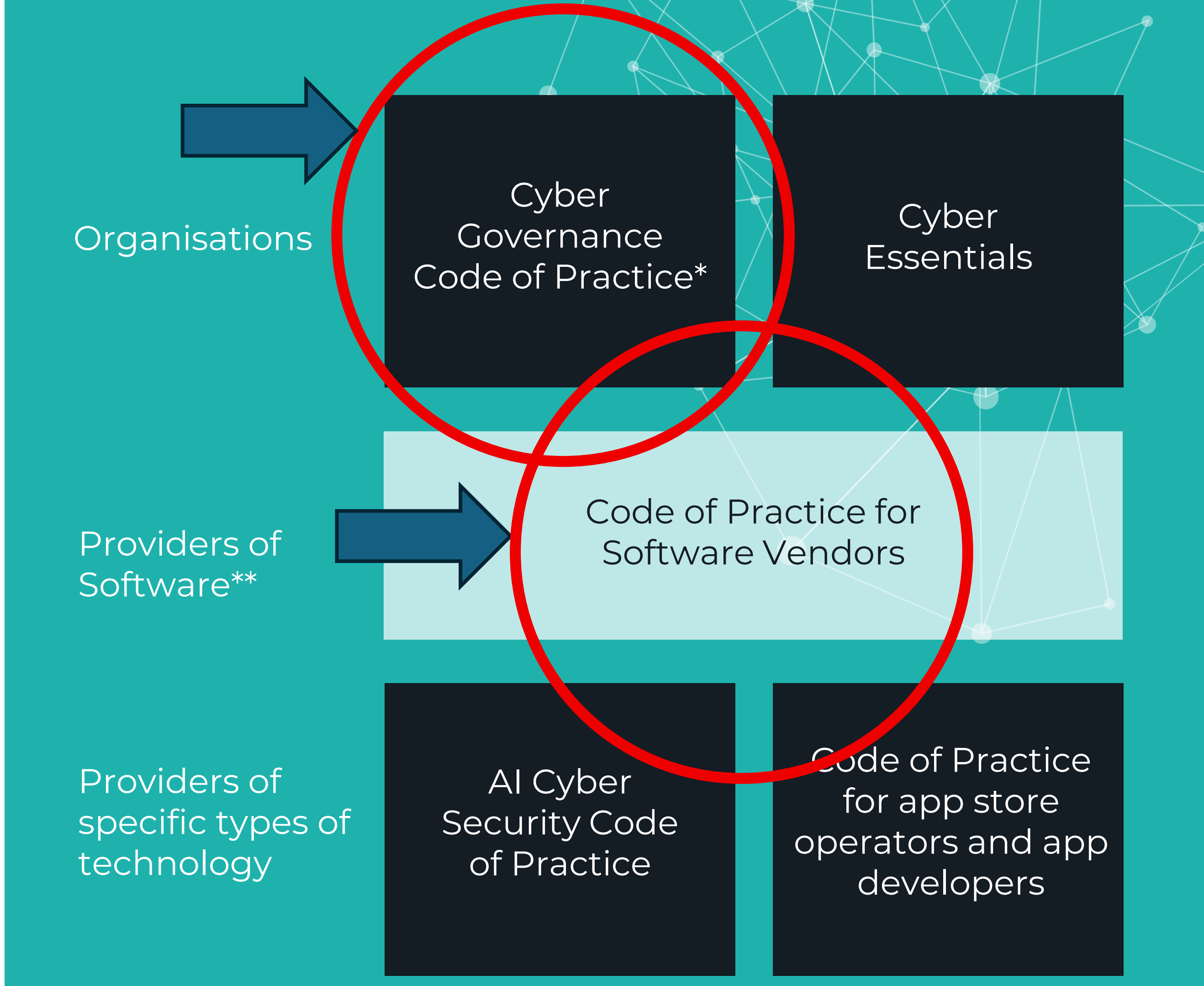
- Software Security

  Software Vendors

- AI Cyber Security

  Vendors using or developing AI

- App Store Operators and app developers
- Consumer IoT Security


Organisations
Cyber Governance Code of Practice*
Cyber Essentials
Providers of Software**
Code of Practice for Software Vendors
Providers of specific types of technology
AI Cyber Security Code of Practice
Code of Practice for app store operators and app developers

*for medium and large organisations, as well as small tech/AI organisation

**including goods and services that contain software

Cyber Governance Code of Practice

Purpose of the Cyber Governance Code

Target Audience

The Cyber Governance Code is designed specifically for board members of medium and large organisations.

Organisational Scope

The code focuses on medium and large organisations, plus small tech focused organisations.

Purpose and Actions

It outlines essential actions boards should take to strengthen cyber governance and risk management.

Government materials supporting the Code

Cyber Governance Code of Practice

Defines the actions boards should take to strengthen cyber governance and security practices.

Cyber Governance Training

Explains why and how board members should implement cyber governance actions effectively.

Cyber Security Toolkit

Provides practical tools and resources to support boards in executing the Code of Practice.

Principles:

Risk Management

The board should

1. Ensure **what** needs to be protected is identified
2. Agree **ownership** of cyber risks
3. Define cyber **risk appetite**
4. Ensure **suppliers** are assessed appropriate to risk
5. Ensure **risk assessments** are performed

Principles:

Strategy

The board should

1. Align cyber with business strategy
2. Ensure strategy aligns with **current risks and obligations**
3. Ensure **resources** are allocated
4. Ensure the strategy **delivers outcomes**

Principles: **People**

The board should

1. Promote a shared responsibility **cybersecurity culture**
2. Gain assurances that there are **clear policies** that support that culture
3. Undertake **training** from the board down
4. Gain assurance that that training is **effective**

Principles:

Incident Planning, Response, Recovery

The board should

1. Ensure there is an **incident response plan**
2. Ensure the **plan is exercised** regularly
3. Take responsibility at the board for **regulatory reporting**
4. Learn from Cyber Incidents and Near Misses

Principles:

Assurance & Oversight

The board should

1. Ensure cyber is governed, with clear **roles and responsibilities**
2. Require **formal reporting** at least quarterly
3. **Communicate** regularly with senior execs, including CISO.
4. Ensure that cyber is integrated in internal audit.
5. Ensure senior execs are aware of regulatory obligations and codes of practice.

Common weaknesses

Cyber Viewed as IT Only

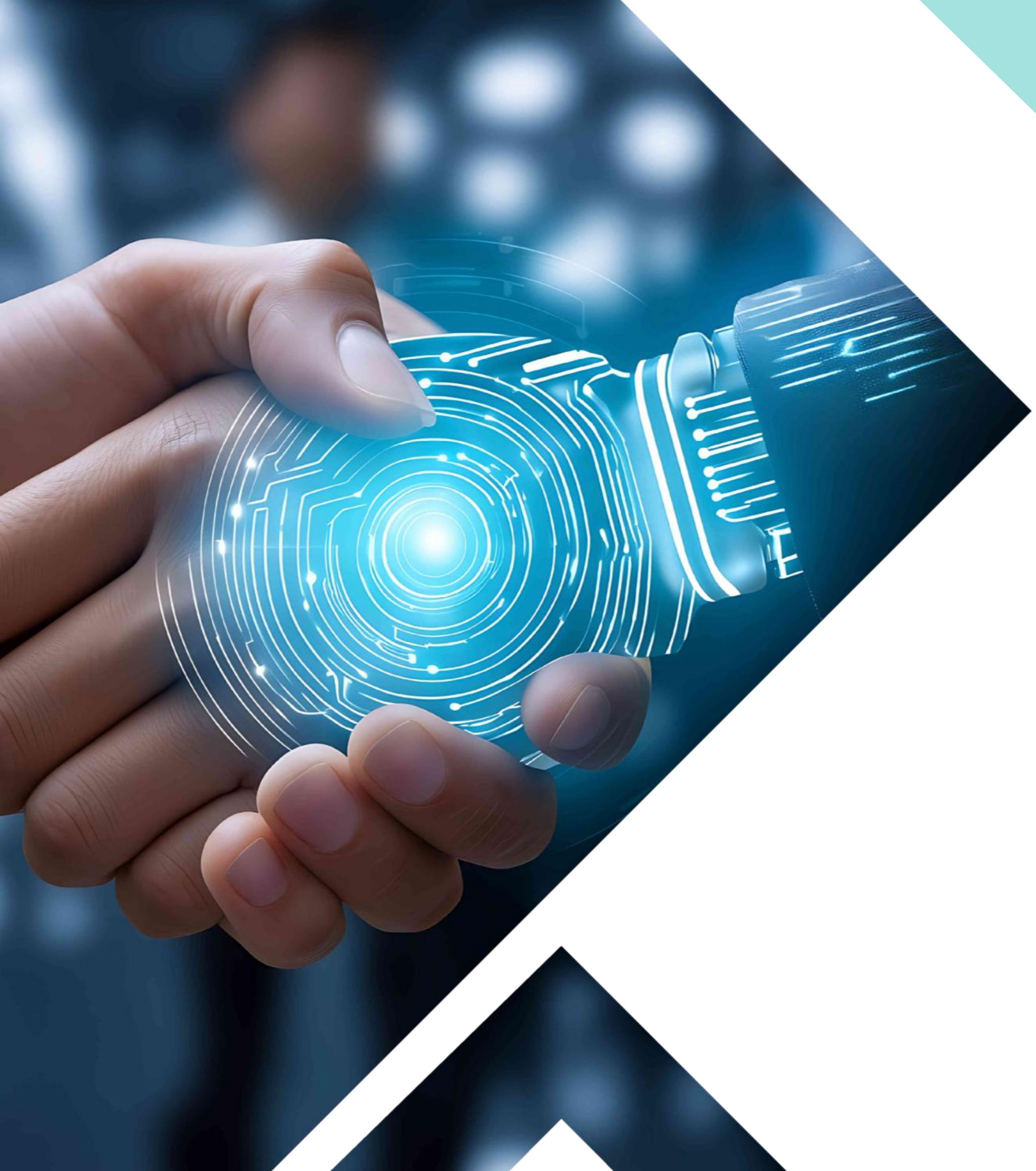
Treating cyber security solely as an IT issue creates gaps in physical security and internal risk management.

Outsourcing Risks Overlooked

Relying on outsourced IT can miss risks from physical premises, other cloud services, and SaaS providers.

Not assessing the supply chain

Data is stored in supplier systems and the risks have not been assessed.



Actions for you

Review your Risks

Create or review your cyber risk register, checking that it considers all critical technology, processes and suppliers.

Test your Incident Response

Run a tabletop exercise with those responsible for incident response to test your plans. How would you detect and respond to an attack?

Review progress on your strategy

Review your risk mitigation plans and cyber strategy to make sure it is pragmatic, realistic and supports your business objectives.

Software Security Code of Practice

Purpose of the Software Security Code of Practice:

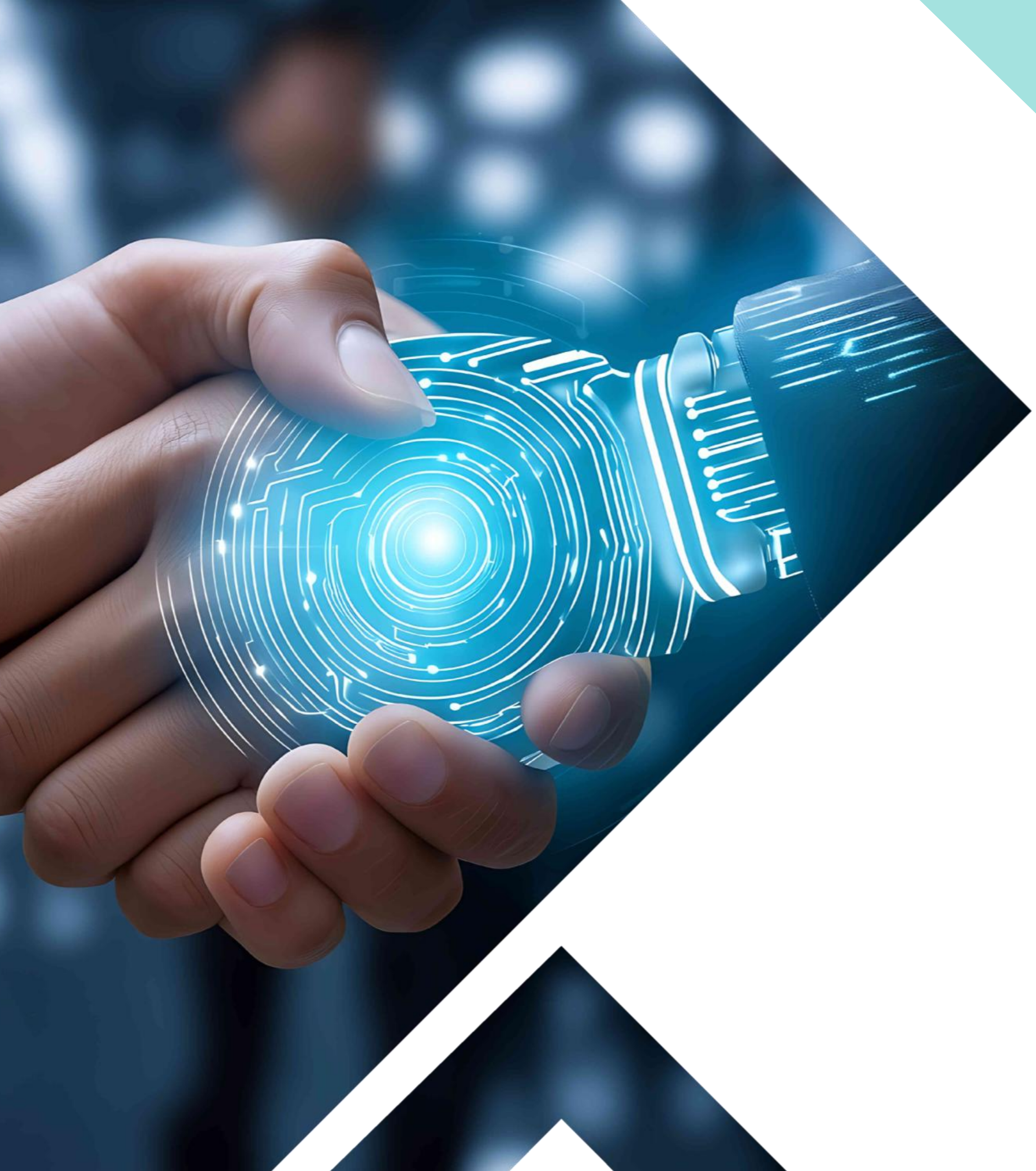
"[It] sets out the fundamental security and resilience measures that should be reasonably be expected from all organisations that develop and/or sell software to businesses or other organisations"

Companies

- Software vendors,
- SaaS providers
- IoT product developers.

Roles

- Senior Leaders
- Technical Specialists
- Procurement Teams



Sources

Expertise from NCSC

The development was guided by expert knowledge from the National Cyber Security Centre.

Industry and Academic Experts

Input was gathered from both industry leaders and academic researchers to ensure comprehensive insights.

Best Practices from Regulations

Incorporates best practices from the EU Cyber Resilience Act and US Secure Software Development frameworks.

Core Principles:

Secure Design and Development

The board should

1. Follow a secure development framework
2. Assess risks associated with third party components
3. Test software
4. Secure by Design and by Default

Core Principles:

Build Environment Security

The board should

1. Protect the build environment

2. Control and log changes to the build environment

Core Principles:

Secure deployment and maintenance

The board should

1. Distribute software securely
2. Have a Vulnerability Disclosure process
3. Detect and manage vulnerabilities
4. Report vulnerabilities (where appropriate)
5. Provide security updates to customers

Core Principles:

Communication with customers

The board should

1. Inform the customer of the support/maintenance provided
2. Provide >1 year EOL announcements
3. Inform customers of significant incidents

Common weaknesses in software security practices

Unsecured Development Environments

Development and build environments are often unprotected and lack proper monitoring compared to production.

Lack of Training and Methodology

Reliance on informal knowledge leads to absence of structured training and development methodologies.

Vulnerable Dependencies

Use of third-party dependencies without proper security checks introduces vulnerabilities.

Missing Security Testing

Lack of security testing in the software lifecycle allows critical vulnerabilities to persist.

Actions

Review your developer training

Is your dev team trained on secure coding and your chosen secure development framework?

Review your security testing

Does your testing regime include 3rd party dependencies and validation of secure coding practices?

Secure your build environment

Consider how you'd know if your build environment were compromised.

Conclusion

CyberSecurity governance is now Expected

By publishing these codes of practice the UK Government is setting clear expectations on how UK companies manage Cyber Security Risk

Software Security goes beyond Production

Securing the production environment is not enough by itself. Security practices are required throughout the development lifecycle.

Risk Management and Protection

Following best practices reduces the risk of a cyber attack and sets clear signals that you are protecting customer data.

FOXTECH

THANK YOU!

Scan to try our free Cyber Risk Assessment

0330 2235622

info@foxtrot-technologies.com