The Strategic Framework for a Cyber Resilient Resilient Scotland

2025–2030: Building a digitally secure and resilient nation where opportunity and economic growth thrive.

DigitalNation.scot

The Dual Nature of Our Digital World

The Escalating Threat

In 2024, nearly half of UK businesses suffered a cyber attack or security breach.

Key Risks:

- **AI & machine learning** exploitation
- **Ransomware** threatening public services (healthcare, councils), and supply chain vulnerabilities.

Sources and data points are representative and intended for illustrative purposes based on common industry reports.

The Proactive Weight

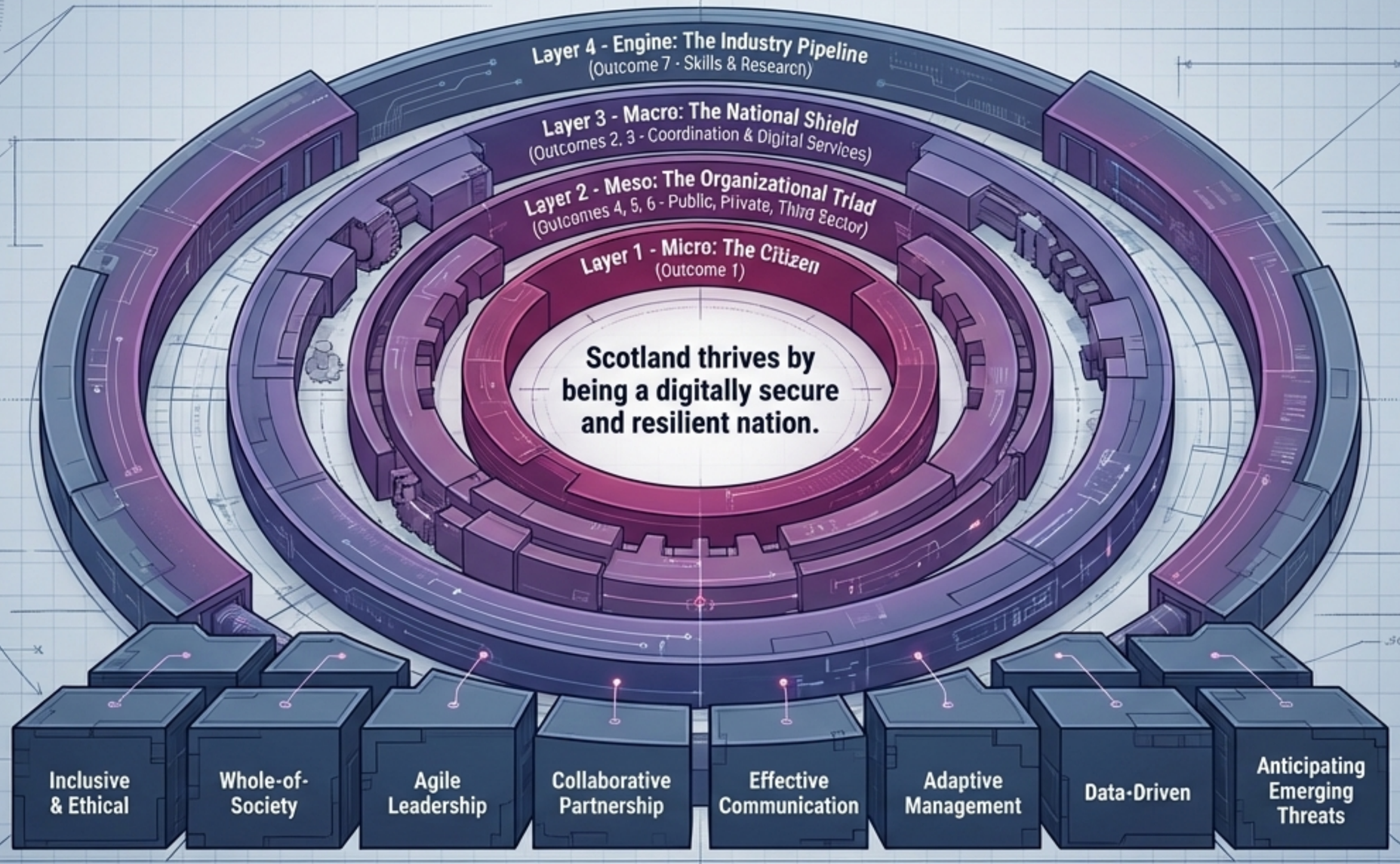
"High-profile attacks are a growing norm. We must shift from reactive fear to proactive readiness."

Key Defenses:

- **Awareness** to recognize threats.
- **Discipline** to reduce risk.
- **Readiness** to respond swiftly.

DigitalNation.scot

The Strategic Architecture of a Secure Nation



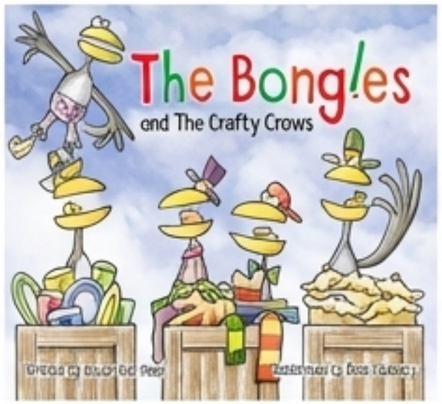
DigitalNation.scot

Layer 1: Empowering the Digital Citizen

Cyber resilience begins with people recognizing risks and feeling prepared to manage them.

Timeline Point 1:
Early Education (Primary 1)

The Bongles and the Crafty Crows: A unique book issued to all Scottish Primary 1 students and libraries in English and Gaelic, introducing basic cyber concepts through storytelling.



Timeline Point 2:
School & College Pathways

Embedding digital hygiene into the curriculum via NCSC's CyberFirst programs.

Timeline Point 3:
Adult Digital Citizenship

Safe online banking, securing smart devices, and protecting personal data in daily digital life.

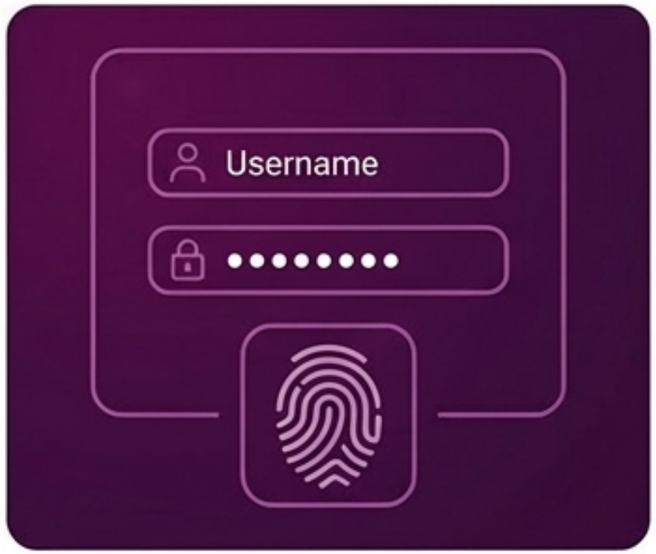
Layer 2: The Organizational Triad

	Public Sector (Outcome 4)	Businesses (Outcome 5)	Third Sector (Outcome 6)
Leadership & Governance	Embedding cyber risk at the board level across all sectors.		
	✓	✓	✓
Incident Readiness	Robust capabilities, regular testing, reporting to Police Scotland/NCSC.		
	✓	✓	✓
Supply Chain Security	Actively managing third-party risks throughout the lifecycle of contracts.		
	✓	✓	✓
Legacy Systems	Identifying outdated software and implementing robust mitigation (network segmentation, audits) where budget constraints delay replacement.		
	✓	✓	✓

Across all sectors, cyber security is no longer just an IT issue; it is a core business risk and leadership priority.

The Toolkit: Tailored Defense Mechanisms

Public Sector: ScotAccount



The secure, simple way to access public services online. Used for PVG scheme disclosures, debt arrangement schemes, and rural registers.

Businesses: Cyber Essentials

NCSC's scheme covering five basic security controls. Certified organizations are 92% less likely to make a cyber insurance claim.

Third Sector: SCVO Tools

Free resources including the Digital Check-up Tool to assess maturity, Incident Response Templates, and quarterly threat bulletins.

The Imperative of ‘Secure by Design’

Path A: Retrofitted Security (The Old Way)

Results in **high maintenance costs, vulnerable legacy systems**, and **difficult scaling.**

Path B: Secure by Design & Default (The Scottish Framework Way)

Systems are **natively resilient to attacks, easier to update, maintain, and scale safely.**

Embedding cyber resilience from the outset of our digital transformation journey ensures our public services are trusted, resilient, and future-ready.

Layer 3: The National Shield

Managing the coordination of a multi-agency response to national incidents.

Scottish Cyber Coordination Centre (SC3)

Providing critical threat intelligence, early warning systems, and managing incident response coordination.

Resilient Digital Public Services

Ensuring the massive amounts of data and connectivity used to tackle urban/rural challenges (traffic, waste, critical infrastructure) remain operational and trusted by the public.

Legacy System Mitigation

Acknowledging the risk of outdated systems in health and manufacturing, requiring immediate segmentation and application controls.

Layer 4: The Economic Engine of Cyber

A Globally Competitive Industry

Positioning the Scottish cyber security industry as an attractive provider of goods and services domestically and internationally.

Academic Excellence & Research

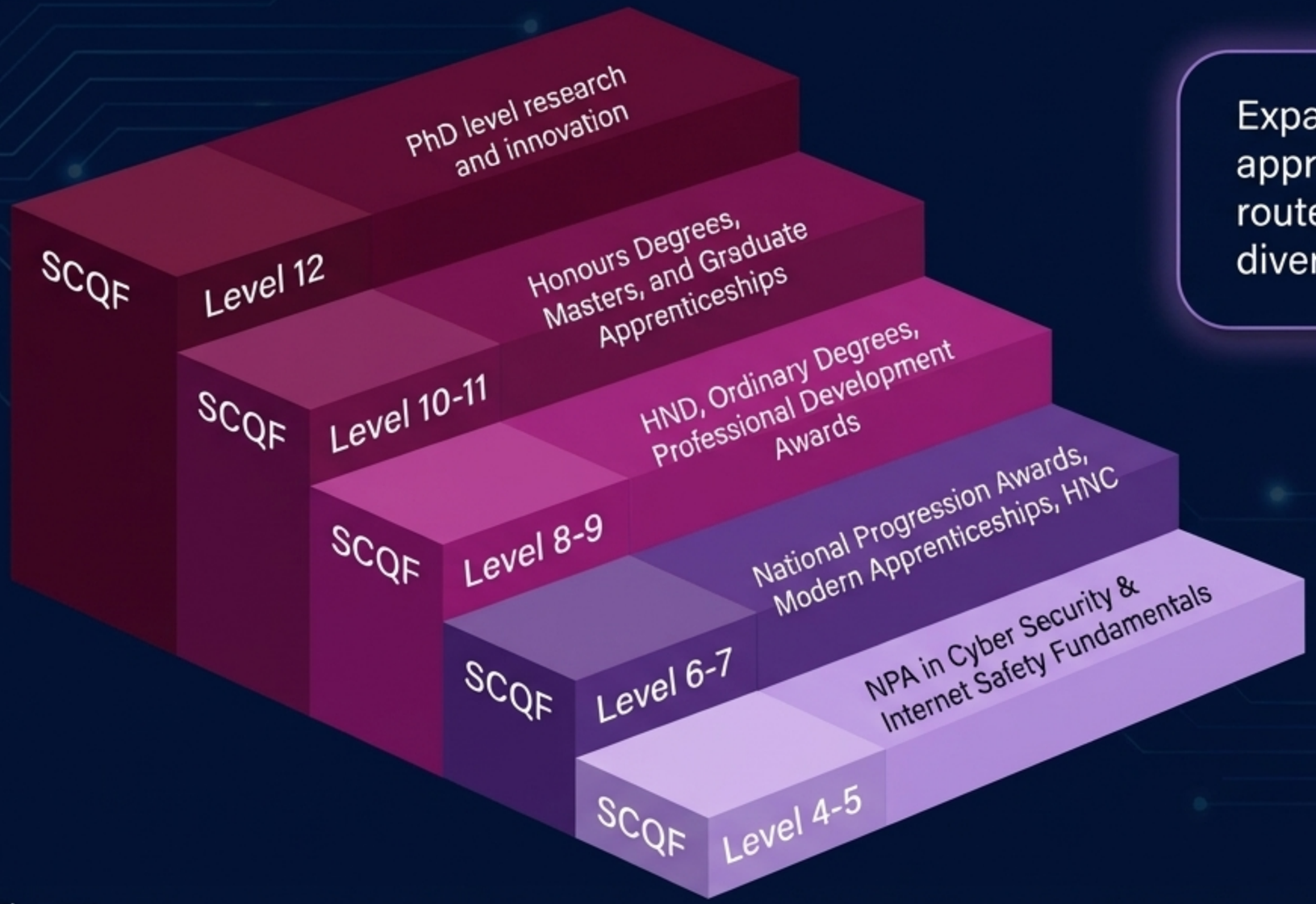
Universities driving innovation to map future challenges and build understanding of emerging tech (AI, quantum computing, machine learning).

Professional Standards

Collaborating with the UK Cyber Security Council to professionalize the workforce, ensuring continuous development and inclusive recruitment.

DigitalNation.scot

Ascending the Cyber Talent Pipeline



Expanding access to apprenticeships, vocational routes, and promoting diversity at all levels.

The Ecosystem in Action: The CyberScotland Partnership

Maximizing collective efforts to avoid duplication, improve early warning intelligence, and drive shared outcomes.

A NATIONAL IMPERATIVE

“Cyber resilience goes beyond securing technologies and systems. Cyber resilience is the ability to prevent, withstand, respond to, recover and learn from, cyber incidents and get the most out of using digital technologies.”

No government can tackle today’s cyber challenges alone. By uniting our strengths across the public, private, and third sectors, we not only protect ourselves—we unlock the economic potential of a bold, modern digital nation.