

The Increasing Cyber Challenge and Good Governance



How strong governance and informed leadership can help organisations navigate rising cyber risks, strengthen resilience, and maintain trust in a digital world.



Giles Grant
CEO
UK Cyber Security Council

Part of the UK's Cyber Security Ecosystem

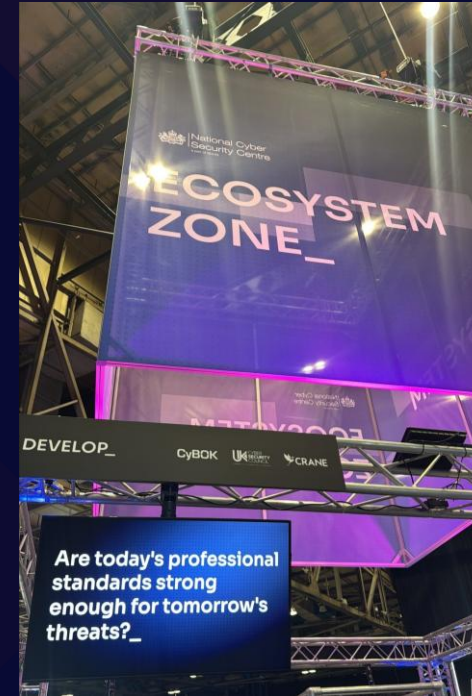


What is the UK Cyber Security Council?

The UK Cyber Security Council is the independent chartered professional body for the UK's Cyber Security Sector under Royal Charter.

We exist to **CONNECT**, **CHAMPION** and **CHARTER** the cyber security profession – all with the goal of making the UK the safest place to life and work online.

Through **setting the standards for industry competence and ethics**, holding the **Cyber Security Professional Register** and **encouraging more people to get into a career in cyber**, we're on a mission to grow and empower the UK's cyber security workforce.



The History of the Council



2016: National Cyber Security Strategy highlighted the need for professionalisation of cyber security.



2016-2021: Project to form UK Cyber Security Council undertaken, involving government, industry, academia and professional bodies from closely related disciplines (Engineering, IT, Information Security).



2021: UK Cyber Security Council granted Royal Charter.



2022: First professionals granted Chartered Cyber Security Professional (ChCSP) title.



2023: Professional registration open to all.

The role of the UKCSC

- **We set the standards for the cyber security profession** through the UK Cyber Security Standard for Professional Competence and Commitment.
- Our Royal Charter status enables us to **award Professional Cyber Security Titles** and hold the UK's Cyber Security Professional Register.
- **We support people to start their career in cyber** providing resources, webinars and networking opportunities to demystify routes into and through the sector.
- As the sector's self-regulatory body, **we set codes of ethics and professionalism** and provide other governance and oversight functions where appropriate.
- **We share knowledge across the sector** bringing together thought leaders, running insightful events and connecting professionals with employers.

Raising the National Baseline:

The UKCSC Mission: To professionalize the workforce through national standards in competence and ethics.

- **Why it is Mission-Critical Now:**

- **Tooling vs Defence:** Agentic AI outpaces manual defence.
- **Systemic Risk:** JLR, British Library, and NHS breaches prove cyber is a national capability issue. Secondary impacts - Supply Chain Risk.
- **Simplifying Trust:** Common standards reduce systemic risk in Critical National Infrastructure (CNI) and procurement.
- **Accountability:** Ethical AI practice requires a visible, competent workforce.

UKCSC Professional Registration = UK Economic and Democratic Resilience

The Increasing Cyber Challenge and Good Governance

How strong governance and informed leadership can help organisations navigate rising cyber risks, strengthen resilience, and maintain trust in a digital world.



The Cyber Challenge Has Changed

Cyber security is no longer a technical problem. It is a leadership challenge

- Every organisation is now a digital organisation
- Cyber attacks affect operations, finances, reputation and public trust
- AI is accelerating both opportunity and risk
- Adversaries are increasingly organised, commercialised and persistent
- Cyber resilience has become a board-level responsibility

Marks & Spencer 2025 Cyber Incident

- Operational disruption
- Supply chain impact
- Customer implications
- Significant media scrutiny

Governance Matters More Than Technology

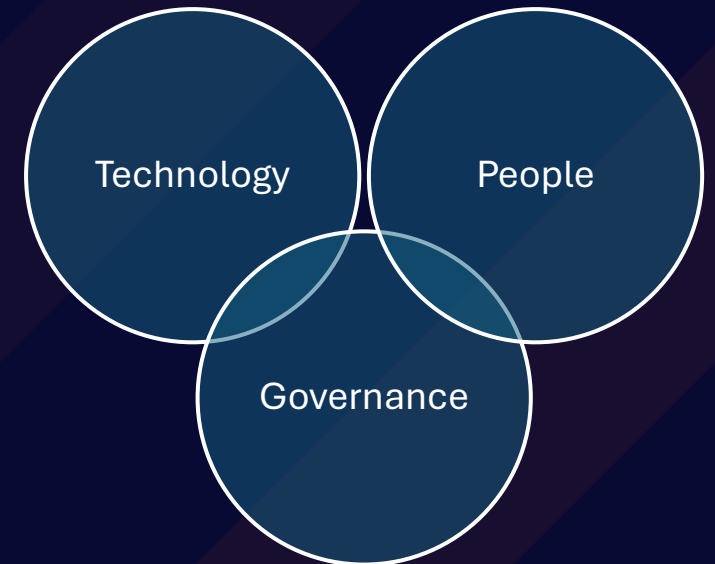
Technology alone cannot solve cyber risk

- Most major incidents involve people, process and decision-making failures
- Governance determines priorities and investment
- Boards establish organisational risk appetite
- Leaders must understand cyber risks in business terms
- Good governance drives resilience



A company may spend millions on security technology but still fail because:

- No incident response plan
- Poor executive oversight
- Weak supplier governance



What Good Cyber Governance Looks Like

Cyber resilience begins with leadership

- Cyber discussed routinely at board meetings
- Clear accountability at executive level
- Defined risk ownership
- Regular reporting and assurance
- Exercised crisis management plans
- Supplier and third-party oversight

Question every Board should ask:

"What is our greatest cyber risk and are we comfortable with it?"

If nobody can answer, governance is probably weak.

The Skills Challenge Behind the Governance Challenge

You cannot govern what you do not understand

- Cyber skills shortages remain significant
- Demand is expanding beyond traditional security roles
- Frontier AI, OT, cloud, quantum and digital trust skills are emerging
- Leaders need cyber literacy
- Professionals need recognised competence pathways



Today's cyber workforce may include:

- Security testers
- AI assurance specialists
- Security architects
- Incident responders
- Digital trust professionals

Many existing frameworks were not designed for these roles.

Professionalisation Is Becoming Essential

Trust requires standards

- The cyber profession is maturing
- Employers need confidence in capability
- Professional registration supports consistency
- Competence should be demonstrable
- Ethical practice must underpin technical excellence



Consider:

- Engineering professions
- Accountancy professions
- Medical professions

All benefit from recognised standards, professional conduct and continuous development.

Cyber is moving in the same direction.

The AI Governance Challenge

AI is creating entirely new governance questions.

- AI can improve productivity and innovation
- AI can scale cyber attacks
- Governance frameworks are still emerging
- Boards must understand AI-related risks
- Cyber, data and ethics must work together



An employee uses a public GenAI platform:

- Sensitive information uploaded
- Intellectual property exposed
- Compliance implications arise

The challenge is not technology.
It is governance.

Why Membership Organisations Matter

Membership organisations are uniquely positioned to influence change

- Trusted by members
- Shape professional standards
- Influence behaviours
- Deliver training and CPD
- Convene industry leaders
- Promote ethical practice



Professional bodies helped drive:

- Health and Safety standards
- Financial governance standards
- Professional qualifications

They can do the same for cyber resilience.

Practical Actions for Membership Organisations

Every organisation can take meaningful action now

- Include cyber risk within governance training
- Build cyber literacy programmes for leaders
- Encourage professional development
- Review supplier and partner risks
- Promote cyber awareness across member communities
- Embed cyber into organisational strategy



Questions to ask your members:

- Do you discuss cyber risk at board level?
- Do you know your critical assets?
- Have you exercised your incident plan in the last year?

Building Trust Through Competence

The future is about trust, competence and accountability

- Digital trust is becoming a competitive advantage
- Professional capability underpins resilience
- Competence must be measurable
- Leadership capability matters as much as technical capability
- Organisations that invest in skills build stronger resilience



Customers increasingly choose organisations that can demonstrate:

- Security
- Trustworthiness
- Responsible use of technology

A **Collective Responsibility**

Cyber resilience cannot be achieved by any one organization.

- Government has a role
- Industry has a role
- Professional bodies have a role
- Academia has a role
- Every leader has a role



**Good cyber governance is not about preventing every incident.
It is about ensuring organisations have the leadership, skills, professionalism and
resilience to respond, recover and maintain trust.**

Solutions – What You Can Do

- **Professionalise Your Teams:** Align and train your security workforce with UKCSC Charters and standards. Join us as an organisation.
- **Train Your Boards:** Ensure leadership understands the systemic nature of cyber risk in the Grey Zone. **Rehearse & roll play.**
- **Build resilience:** Public & Private sector – accelerate & automate patching programs, ensure access to best-in-class protections to mitigate exposure, establish structural containment, need for near-real-time detection & response.

Solutions – What You Can Do

- **Professionalise Your Teams:** Align and train your security workforce with UKCSC Charters and standards.



Solutions – What You Can Do

- **UKCSC Corporate Membership:** Join us as an organisation.



Solutions – What You Can Do



Cyber Essentials



**Cyber Security Toolkit
for Boards**

**Thank You
&
Any Questions?**

UK Cyber Security Council

