ETSI Security Conference 2025

Skills past, present and future

Ian McCormack

National Cyber Security Centre

06/10/2025

National Cyber Security Centre
a part of GCHQ

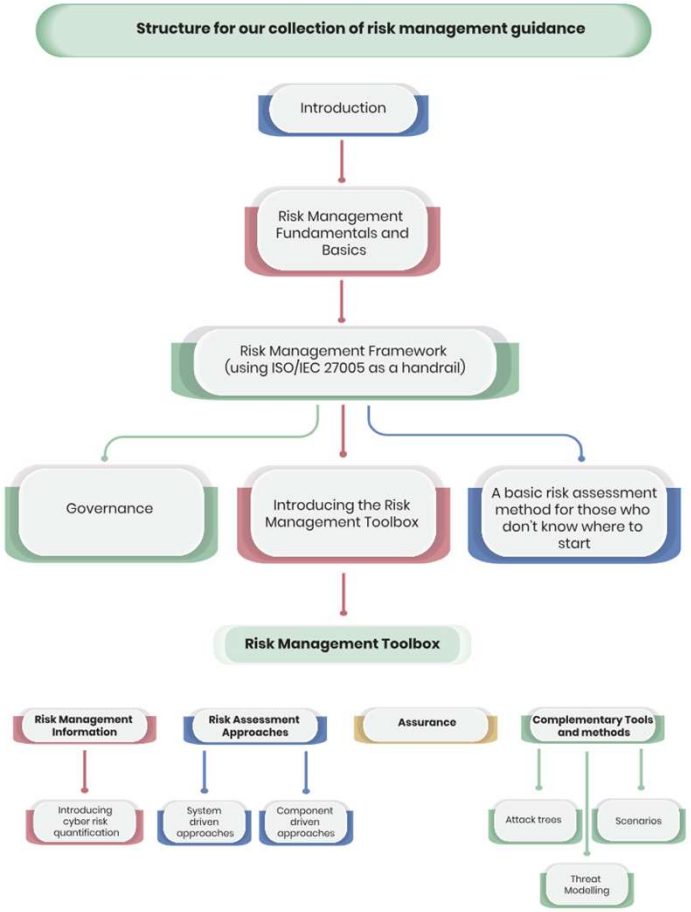
Past

- Compliance; pre-determined assumptions
- Component based approaches (threat x vuln x impact)
- Security frequently not contextualised

National Cyber Security Centre
a part of GCHQ

Skills evolution

- **Re-establishment of fundamental risk-based skills**
- **Greater focus on technical literacy**



National Cyber Security Centre
a part of GCHQ

Present – a few themes

- **Threat environment evolution and fundamental resilience**
- **Incentives, security by design, policy and regulation**
- **Emerging / future technologies, global tech ecosystem**

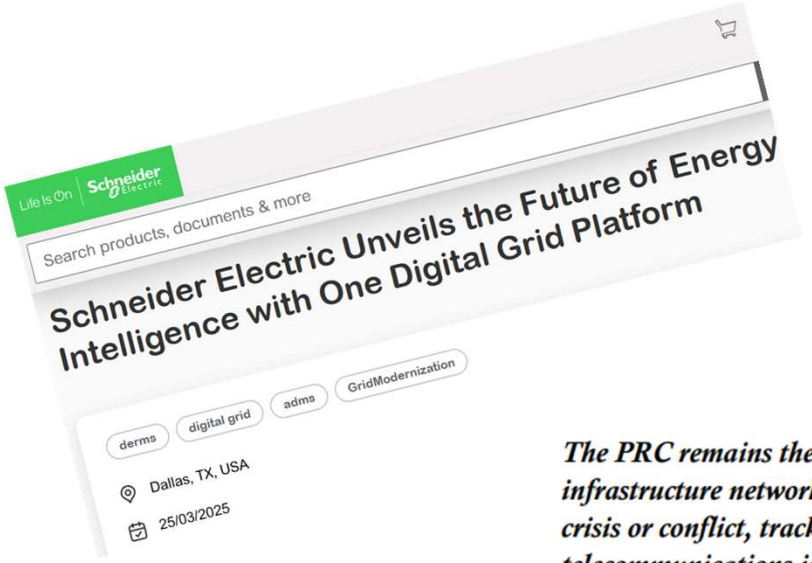
National Cyber Security Centre
a part of GCHQ

Skills evolution

- **Extended enterprise of ‘high-end’ skills**
- **Greater focus on underpinning technology [and sociotechnical] skill**
- **Role of allied professions, functions and the board room become ever more critical**

National Cyber Security Centre
a part of GCHQ

Future



- Complexity and sophistication of threat
- Societal reliance on technologies including AI

The PRC remains the most active and persistent cyber threat to U.S. government, private-sector, and critical infrastructure networks. The PRC's campaign to preposition access on critical infrastructure for attacks during crisis or conflict, tracked publicly as Volt Typhoon, and its more recently identified compromise of U.S. telecommunications infrastructure, also referred to as Salt Typhoon, demonstrates the growing breadth and depth of the PRC's capabilities to compromise U.S. infrastructure.

US ODNI Annual Threat Assessment 2025

National Cyber Security Centre
a part of GCHQ

AI and cyber

Security of AI, adversarial and defensive use of AI

Vulnerability discovery

Agentic red teaming

Security testing

Tooling and attacker capability uplift

Compliance

Leverage of the information environment

Automation and tooling for defenders

Complex attack surface

Frequency and intensity of threat

Agent based blue teams

National Cyber Security Centre
a part of GCHQ

What this could mean for skills

- **Redefined roles**
- **Automation of routine tasks**
- **Focus on more advanced skills**
- **Expert interpretation of AI output**
- **Operation cyber : red / blue**
- **Level of abstraction can make skills development hard**

⚖️ **Summary: The Future Cybersecurity Workforce**

Role Type	AI Impact	Human Role
Entry-Level SOC Analyst	Mostly automated	Oversight & escalation
Compliance Auditor	Partially automated	Governance & interpretation
Penetration Tester	Augmented by AI	Creative exploitation
AI Security Specialist	Emerging	Model validation & threat modeling
Threat Hunter	Enhanced by AI	Strategic analysis
GRC Specialist	Supported by AI	Policy mapping & risk strategy

Generated by Copilot

National Cyber Security Centre
a part of GCHQ

Past, present, future

Plus ça change, plus c'est la même chose

Thank you