IEA Digitalisation & Energy Workshop

Digital Resilience
Digital Resilience -

Best practice in governance arrangements to promote digital resilience

MikeC@CognitioVires.UK
Key components

- We can talk about National & International responsibilities during the discussion session...
- It’s YOUR business, so YOUR responsibility to provide good governance at Board level
- Develop a security culture, with sound and practical policies through:
  - Understanding your business
  - Understanding the threat and vulnerabilities
  - Understanding threat and vulnerability mitigations
  - Constantly applying and revising these parameters through Education, Exercises and Red Teaming
Understanding your business
Understanding your business

Data & Information Infrastructure: Configuration Management Database.

System Data Flow Analysis: Identification of critical assets and the monitoring requirements for those assets.

Physical Infrastructure: Knowledge of where all the physical infrastructure elements are contained that support Enterprise Cyber Operations, both internal and external.
Understanding the threat and vulnerabilities

- Destructive malware
- Worms & virus
- Extortion and theft
- Ransomware
- Whaling
- Rootkits

- Consider the complexity of the range of threat actors:
  - both State and Non-State actors
  - including consideration of realistic numbers

- These actors can be:
  - Witting & Malicious
  - Witting and Non-Malicious
  - Unwitting & Non-Malicious
Understanding threat and vulnerability mitigations

• Technical Measures e.g.
  – E-mail monitoring by volume and content
  – E-mail language analysis
    • Psycholinguistic profiling
  – Total Content Threat Removal
  – Counter-cultural behaviour

• Mitigation by Security Culture
  – Exercise & Red Teaming
  – Vetting & good recruitment practices
  – Application of Cyber Essentials scheme

• Mitigation by Complex, Active Measures
Mitigation by Complex, Active Measures

CII: Critical Information Infrastructure

Red Team your facilities – and report at Board level

- Interdependency studies
- Threat & Vulnerability analysis
- Understand CII complexity
- Identify attack vectors
- Disseminate mitigations
- Identify attack mitigations
- Embrace Government, Industry & Academia
- Develop routes to secure CII
In conclusion, some concerns for the immediate future....

• Supply chain issues such as corruption in third parties
• Exponentially increasing complexity, connectivity and interdependency of components
• Implications of the Internet of Things
• Sophistication of the Insider Threat
The Active Cyber Defence (ACD) Programme outlines how the NCSC intends to tackle - in a relatively automated way - many of the cyber attacks that hit the UK. The diagram below is not an architecture, so not all these initiatives will be in place at day one.