Energy Networks and Cyber Security – Sustainability and Resilience Through Risk Management

October 2014

Modern Energy Networks – Smart Grids

Good

- Efficient
- Interconnected – internally and with partners, customers and suppliers
- Business and technical benefits

Bad

- Single points of failure
- Large attack surfaces
- Increasing focus for attacker interest
- Interconnected – internally and with partners, customers and suppliers

Technical Characteristics

- Complex and non-homogenous industrial networks
- Close coupling of industrial networks with conventional IP-based business networks
- Consumer interfaces to billing systems etc on business networks through smart metering
- Complex ownership and operator structure
- State advice, influence and regulation
- Wide variance in standards and architecture within discrete industries
- Cost-limited appetite for revolutionary change
- Extensive cooperation between operators

Our Assumptions

- Despite edge and interface defences, the network is compromised
- Modern threats are evident by impact and are hard to detect before actuation
- Detection – situational awareness – is thus vital
- Speed and appropriateness of response is just as vital
- Protection must be layered and extend throughout network
- Cyber risk should be identified, mitigated and managed as all other risks
- The risk owner must be closely involved throughout, whether managing his own risk or having it delivered as a service
- A risk-based approach depends on understanding trust
- Security, properly applied, is an enabling, not a blocking function

Technical Threats

- Hazards:
  - Environmental Accident
  - Negligence
  - Collateral Impact
- Threats:
  - State Actors:
    - Service interruption/damage/destruction
    - Intelligence operations
  - Non-State Actors:
    - Hacking
    - Vandalism
    - Fraud/Theft

Consequent Technical Risks

- Current:
  - Environmental/Accidental – Fukushima, Buncefield etc
  - SCADA/ICS system attack – StuxNet etc – industrial systems
  - “Hacking” attack – business systems, logistics systems, command and control systems
  - Spear phishing etc – business systems

- Developing:
  - Specific SCADA/ICS vulnerability exploitation
  - Attacks via smart meters
  - Attacks on hardened business systems (billing etc) through interfaces with industrial/consumer networks

Technical Risk Mitigation

- Current:
  - Environmental/Accidental –Safety, continuity, emergency response planning, load sharing and balancing between operators
  - SCADA/ICS system attack – specific countermeasures, policy etc
  - “Hacking” attack –conventional IA – edge defences, security intelligence
  - Spear phishing etc – malware detection at entry points, some internal network situational awareness
- Developing:
  - Specific SCADA/ICS vulnerability exploitation – full network situational awareness, targeted interventions, variable trust levels, device-level security
  - Attacks via smart meters – hard interfaces, network situational awareness, individual protection for connected devices
  - Attacks on hardened business systems (billing etc) through interfaces with industrial/consumer networks – cross-domain security planning. Low/high protection, determined and regulated data flows, deep packet inspection etc

Results and Benefits From Risk Mitigation

- Better Assurance – fewer financial losses
- Reduced operational impact through prompt response to events
- Better return on capital investment through reduced operating cost
- Better whole-life asset management
- Increased sustainability of infrastructure investments