Protecting Critical Energy Infrastructure
An international electricity and gas company

- ... based in the UK and north-eastern US
  - We play a vital role in delivering gas and electricity to millions of people safely, reliably and efficiently
- One of the world’s largest investor-owned utilities
- Approximately 19 million industrial, commercial and domestic customers
- Almost 28,000 employees
  - 63% work in the US; 37% work in the UK
We supply electricity to approximately 3.4 million customers in the north-eastern US.
Our Gas Distribution business - UK

- In the UK, our gas distribution business comprises four of the eight regional gas distribution networks in Great Britain
- Owns and operates Britain’s largest distribution business
- Delivers gas to almost 11 million homes and businesses
In the US, our Gas Distribution business consists of gas networks in upstate New York, New York City, Long Island, Massachusetts, New Hampshire and Rhode Island.

Delivers gas to 3.5 million consumers.
In the UK, we provide the transmission of electricity and gas as owner and operator of the high voltage electricity transmission network in England and Wales, the gas national transmission system in Great Britain, electricity interconnector with France and storage facilities for LNG.

We also operate, but do not own, the electricity transmission networks in Scotland.
In the US, we provide the transmission of electricity in the northeastern US as owner and operator of high voltage electricity transmission networks in upstate New York, Massachusetts, Rhode Island, New Hampshire and Vermont.
Our non-regulated businesses

- Our non-regulated businesses and other activities are located mainly in the UK. They either operate in markets related to those of our principal businesses or provide support to our own businesses.
- European interconnectors are a key business.
It is vital to all Nations that critical energy infrastructure is secure, resilient to threats, and also has the ability to recover from any incidents. With the increasing reliance on cyber assets to operate critical infrastructure systems, and the convergence of physical and cyber security concerns.

This presentation will look at

- Regulation
- Why this is an issue
- Key risks
- Our strategy
National Grid’s UK and US security regulation landscape around electricity transmission
So what works?

- If a company in the energy sector is risk mature a regulatory approach may lower its cyber security, as compliance may be seen as a goal in its own right.
- If a company is risk immature compliance is a good thing that will improve security.
- You can be completely NERC compliant whilst being inherently insecure.
Three different Ukrainian distribution companies with different systems targeted at the same time

A prolonged reconnaissance period that allowed them to gain key data

- Remote control of systems
- UPS disabled
- A TDOS attack
- Overwriting firmware
- Killdisk used
The strongest capability of the attackers was not in their choice of tools or in their expertise, but in their capability to perform long-term reconnaissance operations, required to learn the environment and execute a highly synchronised, multistage, multisite attack.

Cyber attacks and cyber crime are on the increase and the energy sector is an important target and it is vulnerable.

Cyber security is a real issue for the energy sector and it needs to act now to improve its security.

This incident alone should ensure that the C suite see cyber security as key concern that requires both investment and a mature strategy.
The technological complexity of managing power systems is increasing and becoming ever more reliant upon IT systems to operate.

Historically operational assets within energy were mechanically operated, this evolved to become electromechanical operation monitored by specialist Operational Technology (OT) systems. Operational technologies have evolved and are now based upon the same standard Information Technology (IT) we have in the office and home.

This convergence of distinctly different operating environments (OT IT) has fundamentally changed the risk landscape, at a time when the threat level is rapidly increasing.
Today

- Organic growth of IT in the OT environment has led to technology silos, limited inventory and almost no configuration management information. This has resulted in limited visibility of equipment health and failure risk.

- Limited visibility of equipment health and risk of failure is a key concern due to the typical life expectancy of IT equipment being considerably less than the engineering assets they support. The continued use of obsolete and insecure assets to support key operational processes

- Standard IT and interconnection to business networks, the internet of things and USB storage creates exposure to the risk of cyber attacks

- The level of exploitation of IT in engineering will grow, driven by initiatives such as SMART grid, Enterprise Asset Management, Advanced Network Control System and Complex Event Processing

The key question is how to deal with complete lifecycle management for IT in the operational / engineering environment...
Risk 1. Embedded Vulnerabilities

- There is a risk that due to the lack of security awareness when purchasing, upgrading and deploying IT and OT assets, that vulnerabilities and malware are introduced.

- Consequences if risk materialises – loss of key systems supporting operations that could significantly impair and impact the ability to manage critical infrastructure.
**Risk 2. Widely Available Vulnerability Data**

- There is a risk that information about the legacy OT technology widely used across industry and how to affect its operation is now available on the internet.

- Consequences if risk materialises – loss of key systems supporting operations that could significantly impair and impact the ability to manage critical infrastructure.

Information about how to hack proprietary insecure protocols like Modbus is now widely available on the internet.
We spend millions protecting IT, but little on the operational technology core to running our businesses. Off the shelf IT is increasingly being introduced into the OT environment and not managed effectively.

Risk 3.
Inappropriate Lifecycle Management

- There is a risk that information technology being widely used by the energy sector in the operational environment is not being managed in an appropriate way.
  - No appropriate IT asset management strategy or process:
    - IT assets do not have a thirty year lifespan, this needs to be factored into both depreciation and investment planning
    - No patching no anti malware protection
    - Little understanding of the threats
    - No defined / managed secure perimeter, the increasing use of wireless / remote IT technology
    - Little coordination between corporate IT managed systems and business managed systems

- Consequences if risk materialises – loss of key systems supporting operations that could significantly impair and impact the ability to manage critical infrastructure.
Risk 4.
IOT / Shared Threats / Standardisation

- Key suppliers are standardising ICS / SCADA technology potentially making it vulnerable to threats targeted elsewhere. There is an increasing risk of system failure due to the increased threat level evidenced by events across the ICS sector, the level of sophistication is increasing on a daily basis with new malware targeting both OT and IT.

- Consequences if risk materialises – loss of key systems supporting operations that could significantly impair and impact the ability to manage critical infrastructure.

Thousands of variants of viruses are made daily, one day a virus will have the right DNA to damage key assets unless they are protected.
Risk 5. Increased connectivity / IOT

- Increasing connectivity and accessibility has elevated the cyber risk to once physically isolated assets. The use of mobile and WI/FI networks, tied to the use of third parties across engineering further compounds this risk; by providing additional points of access to inherently insecure critical assets.

- Consequences if risk materialises – loss of key systems supporting operations that could significantly impair and impact the ability to manage critical infrastructure.

We are opening more doors than we are closing
Critical Infrastructure

- National Grid’s assets are essential for the delivery of energy to homes and businesses across the UK and US.
- The loss or failure of some assets would cause the loss of the energy supply to large numbers of consumers.
- These assets are critical to the UK and US economies and include some of our systems and operational cyber assets.
RTU101

- Rabbit 3000 processor running @ 29.4 mhz
- 4 digital inputs with LED indicators (contact closure type)
- 2 Isolated digital outputs
- Two 4-20 ma analog Inputs
- Two isolated 4-20 ma outputs
- Two RS232 serial ports
- Serial port TX and RX LED’s
- Dedicated programming/diagnostics port
- Standard communication protocols available
- +12v dc powered
- Power-on status LED
- Four status LED’s for various diagnostics
- Custom Programmable in "C"
- 512K flash and SRAM
- 10/100 Base-T ethernet option
- Real-Time clock with Day Light Savings Support
- Quick-connect plugs
- Backplate mounting
Brightwell DB1 RTU

J1 Touchscreen controller

J2 Power (5V DC)
J3 Power (10-30V DC)
J4 Audio
J5 JTAG
J6 10/100BaseTX Ethernet
J7 GPIO
J8 Dual USB host
J9 Camera interface
J10 USB client
J11 Serial port – COM1
J12 64-way PC/104 expansion
J13 40-way PC/104 expansion
J14 LCD panel interface
J15 Serial port – COM2
J16 LCD panel LVDS interface
J17 CAN bus
J18 Serial port (RS422/485)
J19 Serial ports (COM3/4)
J20 CF+ interface
J21 IEEE802.15.4 / ZigBee
J22 SDIO
J23 Wireless interface
J24 Backlight power
Key Points

- The power networks are now reliant on IT to be able to operate, the systems required to run the networks are going to become ever more complicated.
- The attack surface continues to grow.
- The threat of cyber attacks on power networks is increasing.
- A lot of the assets that run the power network cannot be changed without incurring huge costs for a period of several years or longer.
- They are subtly different to standard IT systems and require a bespoke approach to mitigate the risks.
- We have people that understand power networks or cyber security but very few who understand both!
Operational activities across energy networks have become reliant on IT, an independent world of "operational technology" (OT) developed separately from most companies' core IS systems.

IS departments need to engage with OT environments to assess how best to ensure that OT systems are managed effectively and investigate:

- Convergence
- Alignment
- Integration

CULTURAL CHANGE
EVOLVE WITH THE THREAT
Computers can be manipulated in a way that can damage physical plant and hardware. The continued deployment of SCADA and other types of intelligent devices into energy networks expands its notional attack surface, the risk is increasing all the time.

It is vital to all nations that their energy infrastructure is secure, resilient to threats, and also has the ability to recover from any incidents. With the increasing reliance on cyber assets to operate critical infrastructure systems, and the convergence of physical and cyber security concerns, we need to assess the key risks and then mitigate these risks to ensure we have an appropriate balance between risk and cost.
Strategy

• An intelligence led and in-depth threat analytics approach to cyber security risk reduction

• Internally sourced organisation, managing key areas of cyber resilience only outsourced where effective and appropriate

• A trusted partner to the businesses for operational resilience
  • Cyber security seen as a valued asset
  • Seen as a center of excellence for cyber security

If we don’t do the above we will end up with more power outages, leading to regulation that will not adequately secure critical power networks from sophisticated attacks