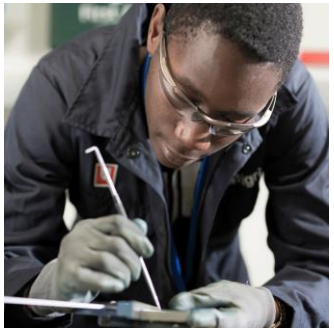
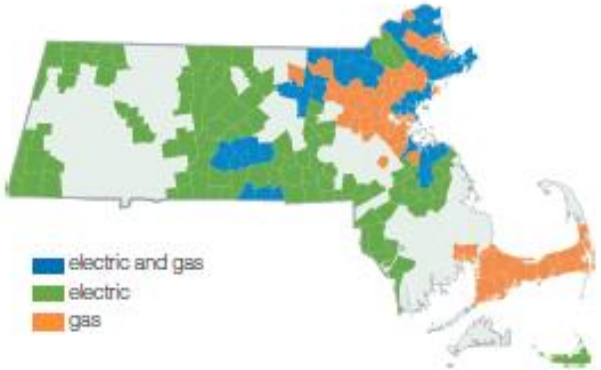
Resilience and Cyber Security

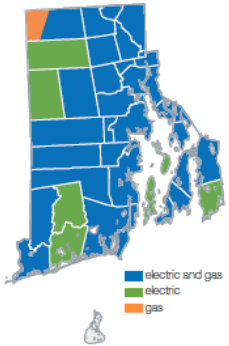


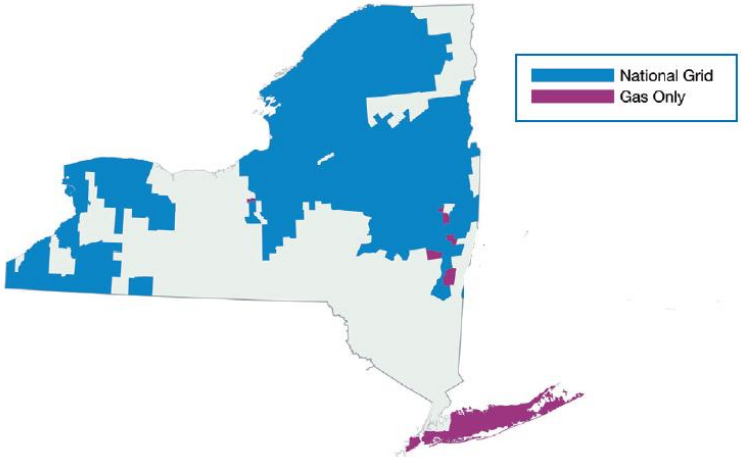
Elaine Wilson
Digital Risk & Security

June 5, 2018

National Grid US







1.3 million
electric customers

876,000
gas customers

486,000
electric customers

257,000
gas customers

1,600,000
electric customers

2,394,000
gas customers

nationalgrid

Changes influencing utilities and cyber security

Change is being driven from many sources and cyber teams must be flexible, applying the right level of controls based on the risk profile

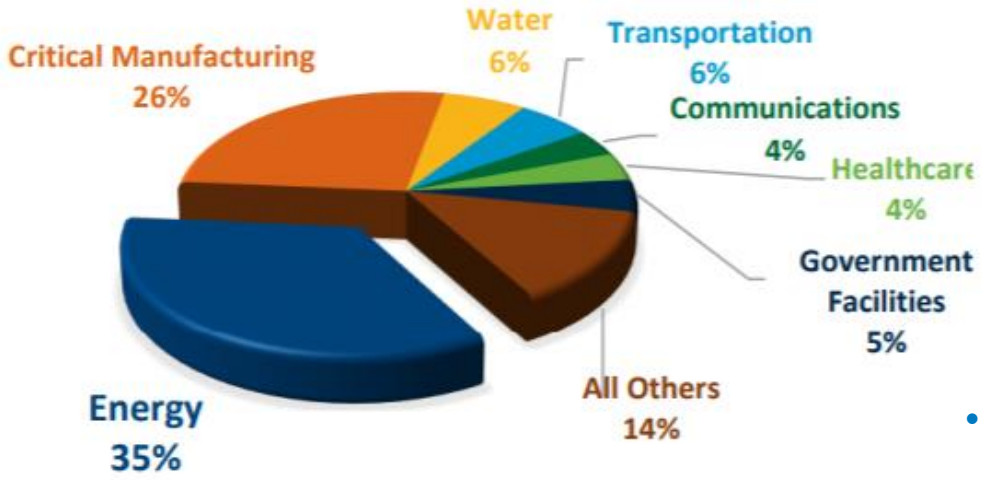
- Analytics
- Application delivery
- Cloud
- Digitization
- Grid modernization
- Information growth
- Internet of things
- IT OT Convergence
- Mobility
- Regulation
- Situational Awareness
- Threats
- Response to weather events

Cyber events can occur at any time

Blue sky days

Storms

The threat is real



- **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reports that the energy sector experienced more cyber incidents than any sector from 2013 to 2015, accounting for 35% of the 796 incidents reported by critical infrastructure sectors.**
- **Despite the sector's ever-improving defenses, the variety of threat actors and methods of attack are expanding, while the impact of incidents has evolved from exploitation to disruption to destruction.**

Source: DoE Multiyear Plan for Energy Sector Cybersecurity, March 2018

nationalgrid

Resiliency and Cyber Security

Core principles:

- **IDENTIFY** what is important;
- **PROTECT** with appropriate risk based controls;
- Ability to **DETECT** incidents and events;
- Be prepared to **RESPOND** and to;
- **RECOVER** what is important in line with agreed timescales and levels of business criticality.

Leverage industry standards & frameworks

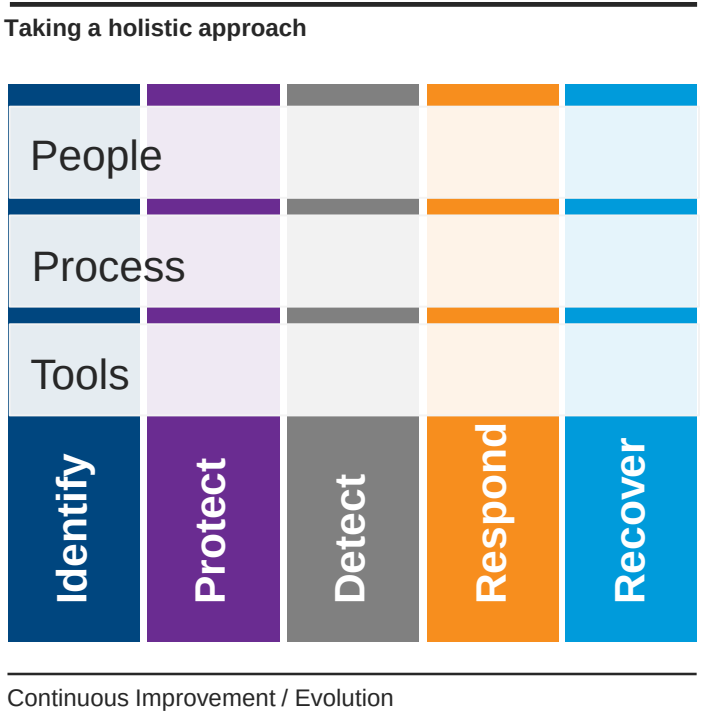
nationalgrid

Apply security services aligned to each function

Identify	Protect	Detect	Respond	Recover
Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Enabling resilience

Approach to resiliency



- People
  - Collaborate
  - Maintain skills
  - Security awareness / training
- Process
  - Maintain processes for continuous improvement
  - Process details communicated and understood
  - Provides speed to respond / deliver
- Tools
  - Right fit tools
  - Multi-layered approach
  - Integrated
  - Reuse

Diligence every day to:

Ensure current and future operations maximize opportunities of emerging technologies, while being resilient to threats

nationalgrid

Contact information
Director, US Security Architecture
elaine.wilson@nationalgrid.com