

## Myth Busting:

### Taking action on Smart Grid Cybersecurity

#### MYTH 1:

“Cyber attacks aren’t a real threat”

The number and range of attacks continues to grow every year.  
Advice: Ensure your organisation and management know about the threats.

#### MYTH 2:

“We (Utilities) are not targets”

In 2015 thousands of consumers in the Ukraine lost power due to a cyber-attack on the energy network.  
Advice: Talk to your peers and try to share intelligence of energy grid incidents.

#### MYTH 3:

“We are not vulnerable”

An attacker will find the weakest point in your defence wherever it is.  
Advice: Many of the defences we have used in the past won’t protect the Smart Grid.

#### MYTH 4:

“We would know if we were breached”

It can take months to discover a breach assuming you can detect it at all.  
Advice: Assume you have been breached and look for the intruders.

#### MYTH 5:

“There is no money to be made in attacking the grid”

Increasingly criminals are using ransom-ware to drive profits from critical infrastructure.  
Advice: Understand the specific threats and the impact they could have on your operations.

#### MYTH 6:

“We have a crisis management plan”

Great. Does it include recognising and responding to a cyber incident?  
Advice: Preparation is key – develop a plan to meet different types of attack.

#### MYTH 7:

“It’s our vendors’ problem”

The ultimate risk lies with the energy operator. Standard contracts rarely address the needs of critical infrastructure.  
Advice: Work with your key suppliers before you have a security incident.

