Issued 4/10/18

Securing Critical Infrastructure in the Wake of Unprecedented Cyber Threats

Last year saw a worrying trend in the cybersecurity attack arena as critical infrastructure came under fire, with many suggesting in 2018 these attacks could escalate. Various defense departments warned of nation-state campaigns targeting operational technology (OT) within the energy sector and nuclear facilities across the globe. In tandem, malware strains such as Industroyer, materialized with claims that they are specifically targeted at critical systems. We've also witnessed events that illustrate the repercussions when attacks are successful – such as the 2017 WannaCry ransomware attack, the 2016 attacks on US water utilities, and the 2015 attack on Ukraine's electricity network. Any successful compromise will have a detrimental effect on the UK's economy with the potential to have an impact on citizen's safety. Recognizing the threat, the UK government is looking to implement the European Union Network and Information Security (NIS) Directive to help make sure UK operators in electricity, transport, water, energy, health and digital infrastructure are prepared to deal with the increasing numbers of cyber threats.