



## Oil & Gas Cyber Security

# Protecting Your Operational Technology (OT) and IT from Cyber-Attack

*Don't risk loss of production, the safety of your people, major pollution and the huge potential cost of a cyber-attack*

Options available to give different levels of protection and recovery:

- Staff Training to reduce human error
- Cyber-attack Response Plan – be ready
- OT & IT protection measures
- 24/7 Monitoring and Response
- Restore data and operations
- NIS Directive compliance
- Facilitate cyber-attack insurance
- Tailor-made subscription services

**The Threat is Real** – the risk of cyber-attack is very high and potentially very damaging. **Statoil, BW Group** and **Rosneft** have all been targeted. In Norway alone, 50 Oil and Energy Companies have fallen victim to hackers.

**Our Team** has worked at the highest level in Government Security Agencies, the Armed Forces and out in the oil and gas industry. We understand the vulnerabilities of IT and the Operational Technology (OT) that operates your facility and keeps it safe.

**The NIS Directive** – are you compliant with the **Network and Information Security Regulation (EU NISD)**, which is now UK law?

Essential services operators in the UK (and Europe) are mandated to protect their infrastructure from cyber-attacks. All serious incidents must be reported to the Competent Authority with severe penalties for non-compliance.



## Oil & Gas Cyber Security

# Cyber Prism Delivering Cyber Security Solutions

### Cyber Risk Management

- Identify Threats
- Document Assets to be protected
- Assess consequences of an attack
- Establish risk tolerance and plan

### Survey & Protection

- Identify & protect IT & critical OT assets
- Systems security and data security
- Networks security: internal & external
- Secure Communications & Encryption

### Incident Monitoring, Response & Restoration

- 24/7 cyber incident monitoring
- Base systems configuration & backup
- Develop Incident Response Procedure
- Restore operations & data expeditiously

### NIS Directive Compliance

- Establish asset register & vulnerabilities
- Specify best fit protection measures
- Monitor networks & detect anomalies
- Response & Recovery planning

### Training & Compliance

- On-site & e-Learning Cyber Training
- Cyber-attack simulation
- Policies & Procedures including social media
- Compliance Reviews & Audits

For more information:  
[www.cyberprism.net](http://www.cyberprism.net)  
[contact@cyberprism.net](mailto:contact@cyberprism.net)