Cyber Risks to the UK’s Energy Infrastructure: Challenges and Opportunities in the Delivery of the Transition

WHY THIS MATTERS NOW

Critical infrastructure is the most targeted sector globally. The scale, frequency, and sophistication of attacks are accelerating — and the consequences extend far beyond data loss.

300%

Rise in OT Ransomware

Increase in ransomware targeting OT/SCADA systems, 2022–2024 (Dragos)

82%

Human Element

Of all breaches involve a human element (IBM Cost of a Data Breach 2023)

15+

Nation-States

Actively targeting the energy sector for espionage and disruption

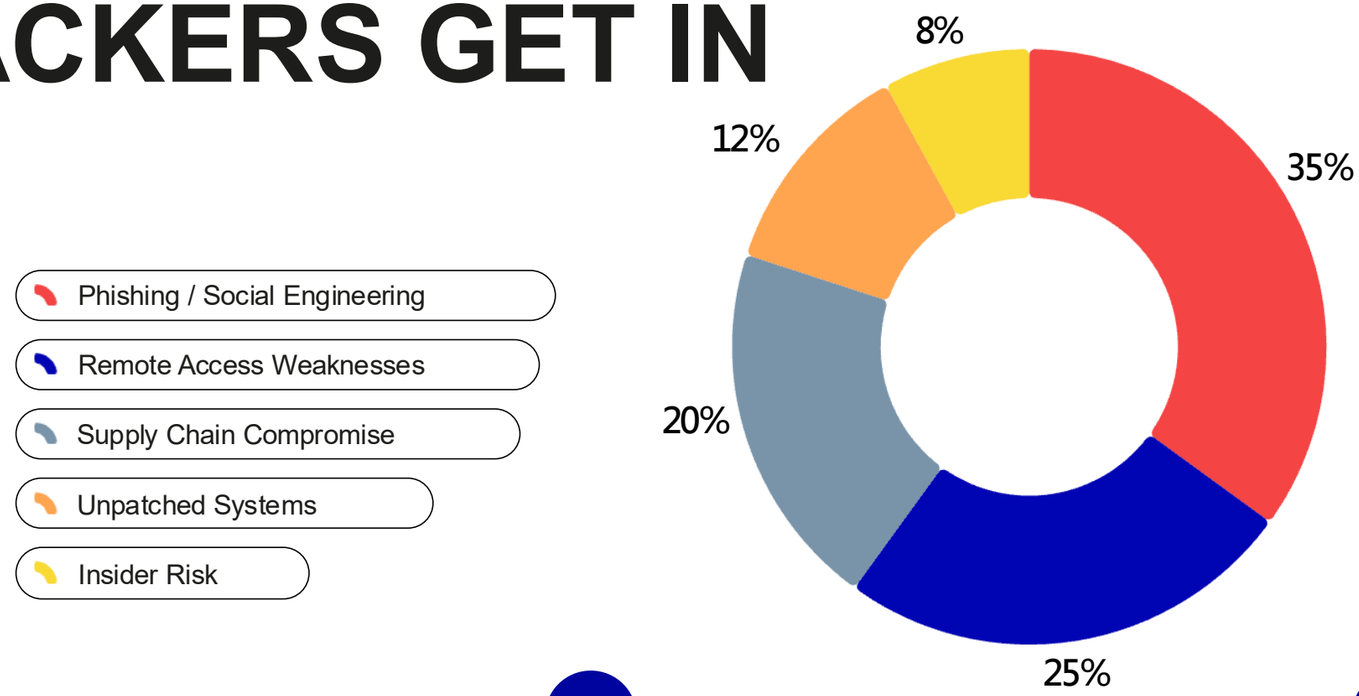
$4.4M

Colonial Pipeline

Ransom paid in 2021 — from a single compromised password with no MFA

UNDERSTANDING THE THREAT: WHO, WHAT & WHY

HOW ATTACKERS GET IN



Phishing & Social Engineering

Entry point for 80%+ of successful breaches, the Ukraine attack started with a single email

Remote Access Weaknesses

VPN without MFA remains the #1 exploited initial access method, Colonial Pipeline root cause

Supply Chain Compromise

Now the #1 fastest-growing attack vector, malicious firmware in renewables equipment and meters

Unpatched Systems

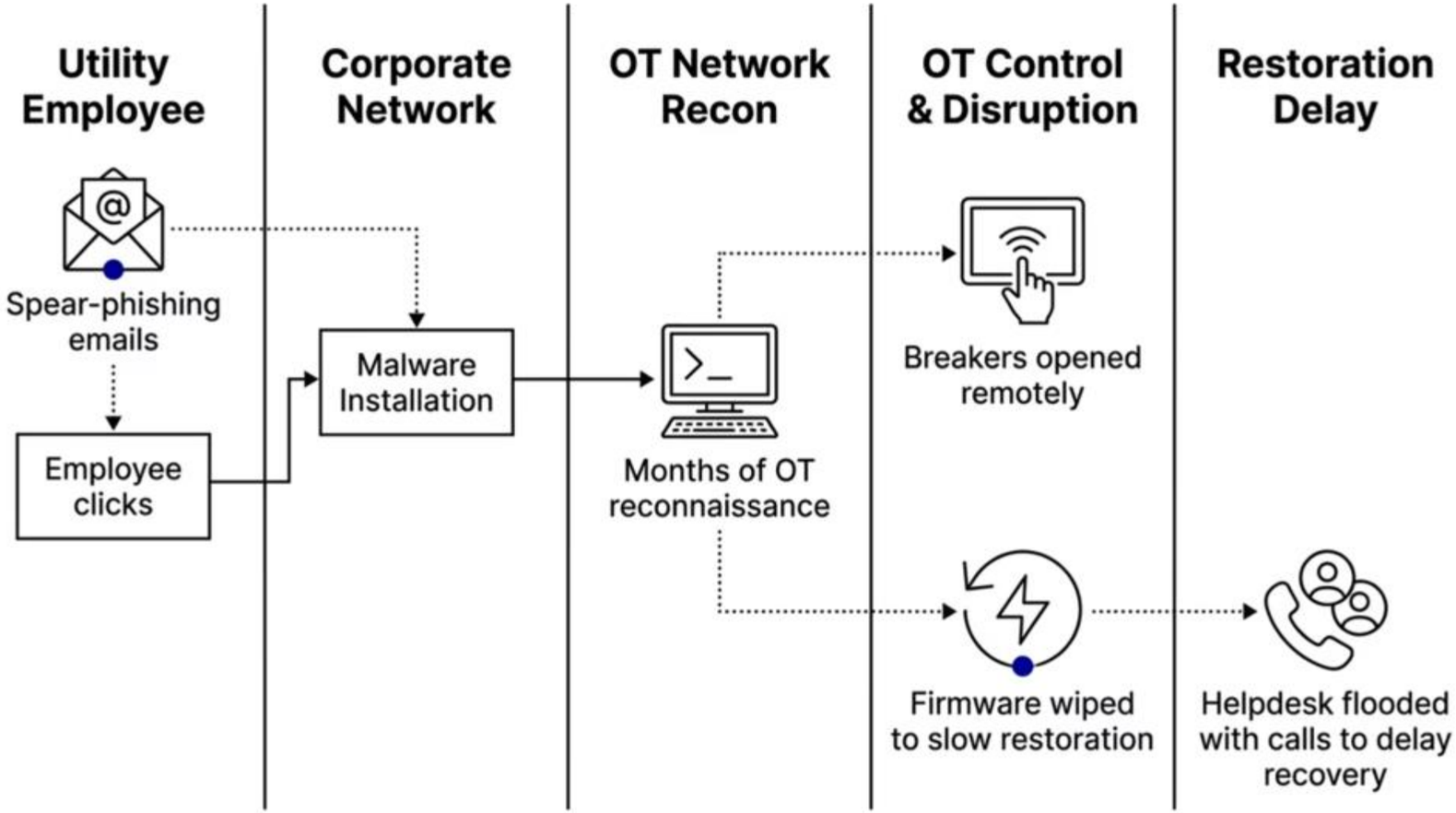
OT systems with 15–30 year lifespans rarely receive timely patches, legacy vulnerabilities persist

Insider Risk

Contractors with persistent, unmonitored access; credentials not revoked after departure

UKRAINE POWER GRID ATTACK. 2015 & 2016

The world's first confirmed cyber-physical attack on a power grid. 230,000 people lost power in winter initiated by a single phishing email.



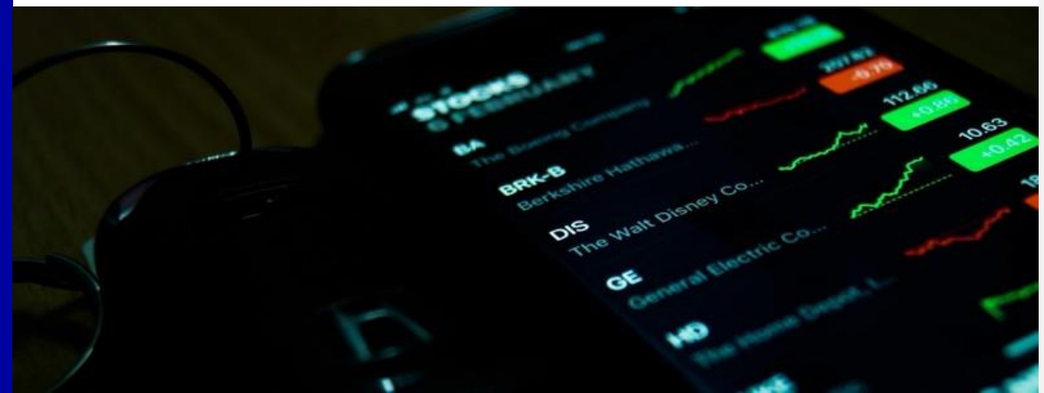
Attacker
Sandworm Group, attributed to Russian military intelligence

Key Lesson
Manual override capability and offline procedures are life-saving investments

Key Lesson
Attackers are patient, they observe and plan for months before striking

JAGUAR LAND ROVER – SUPPLY CHAIN ATTACK

Lesson: Segmentation is vital to limit damage. Need to move towards a Zero Trust approach



DATE & LOCATION

August – September 2025

Shutdown global manufacturing operations, including major UK plants at Solihull, Halewood and Wolverhampton. Impacted over 5000 UK organisations

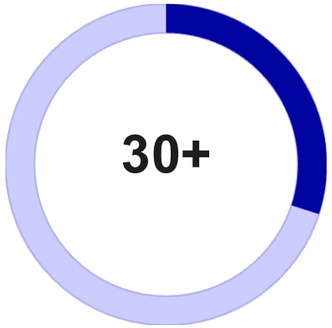
HOW?

- Attackers compromised the **IT Helpdesk to reset credentials**
- Exploited vulnerable version of **SAP Netweaver**
- Lack of segmentation between **IT to OT network**
- Attack claimed by **Scattered Lapsus$ Hunters**
- The second successful cyber attack of JLR in 2025

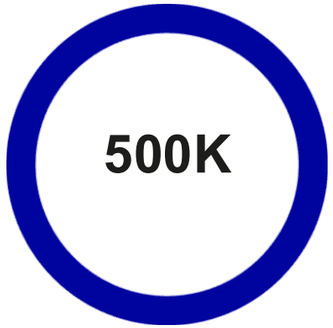
IMPACT

- **Operations halted:** Production halted for **5 weeks**
- **Data Loss: 350Gb** of internal data exfiltrated
- **Economic Costs:** Costliest UK cyber attack so far with **estimated loss of ~£1.9bn**
- **Trust impact:** Breakdown of trust in **software supply chains**

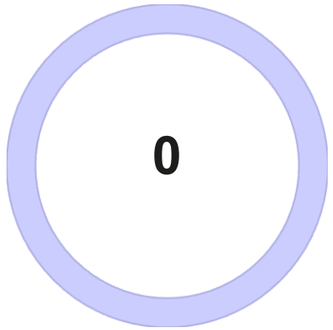
POLAND RENEWABLES WIPER ATTACK. DEC 2025



Wind & solar farms targeted



Heat customers at risk



Blackouts, grid stayed stable

29 Dec AM

Wiper triggered → comms loss at substations

29 Dec PM

CHP attack blocked by EDR/XDR

30 Dec

Containment & forensics

Method

Wiper malware on RTUs, HMIs & edge devices

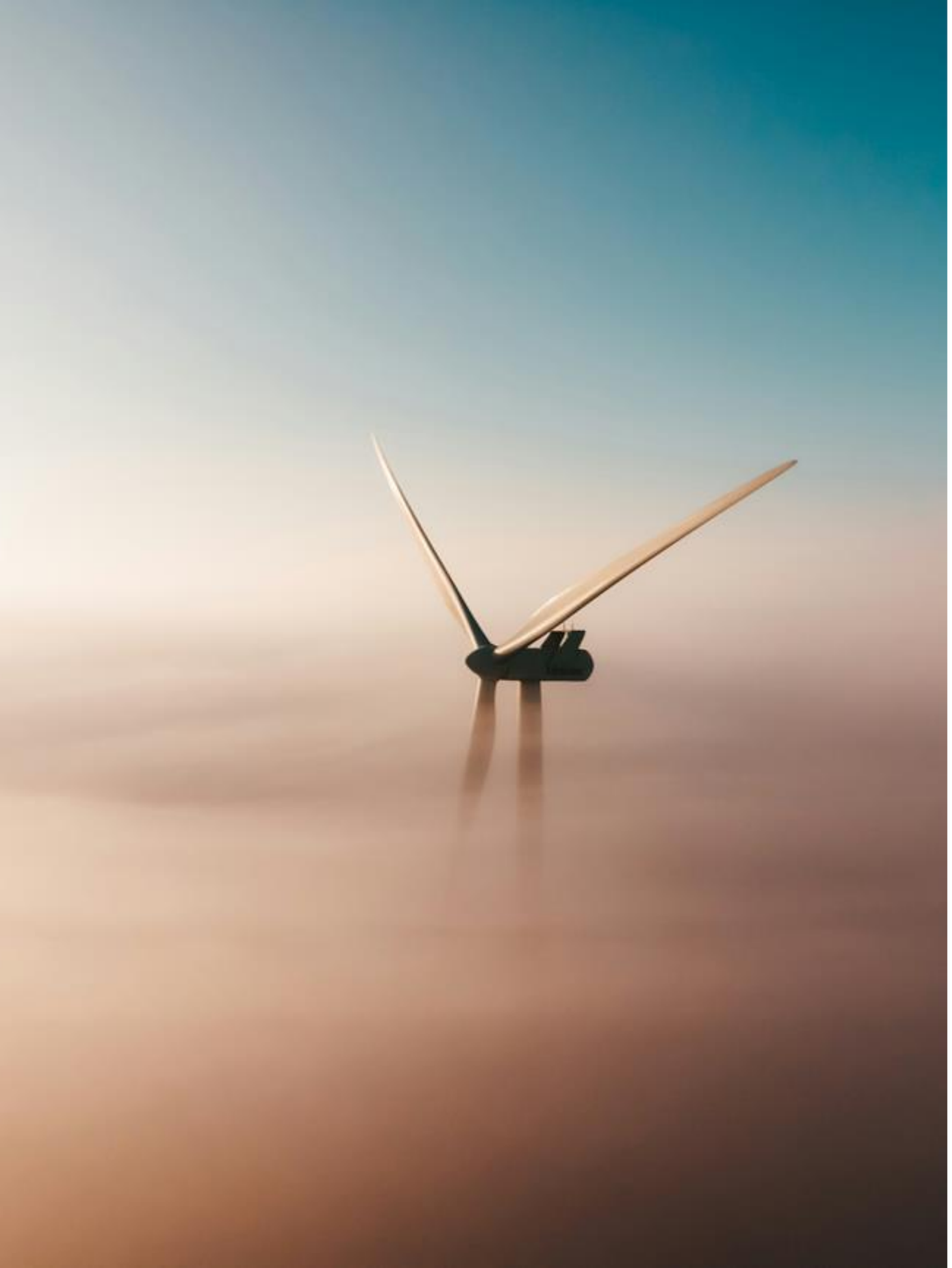
Defense

EDR blocked CHP attack. Heat & power uninterrupted.

Attribution

Sandworm / Static Tundra (Russia-linked)

Sources: CERT Polska (Jan 2026); ESET Research (Jan 2026); CISA Alert (Feb 2026)



Renewables: A Growing & Under-Secured Target

IoT Telemetry Exposure

Sensors and edge devices transmit data over public networks with minimal encryption or authentication

Default Credentials

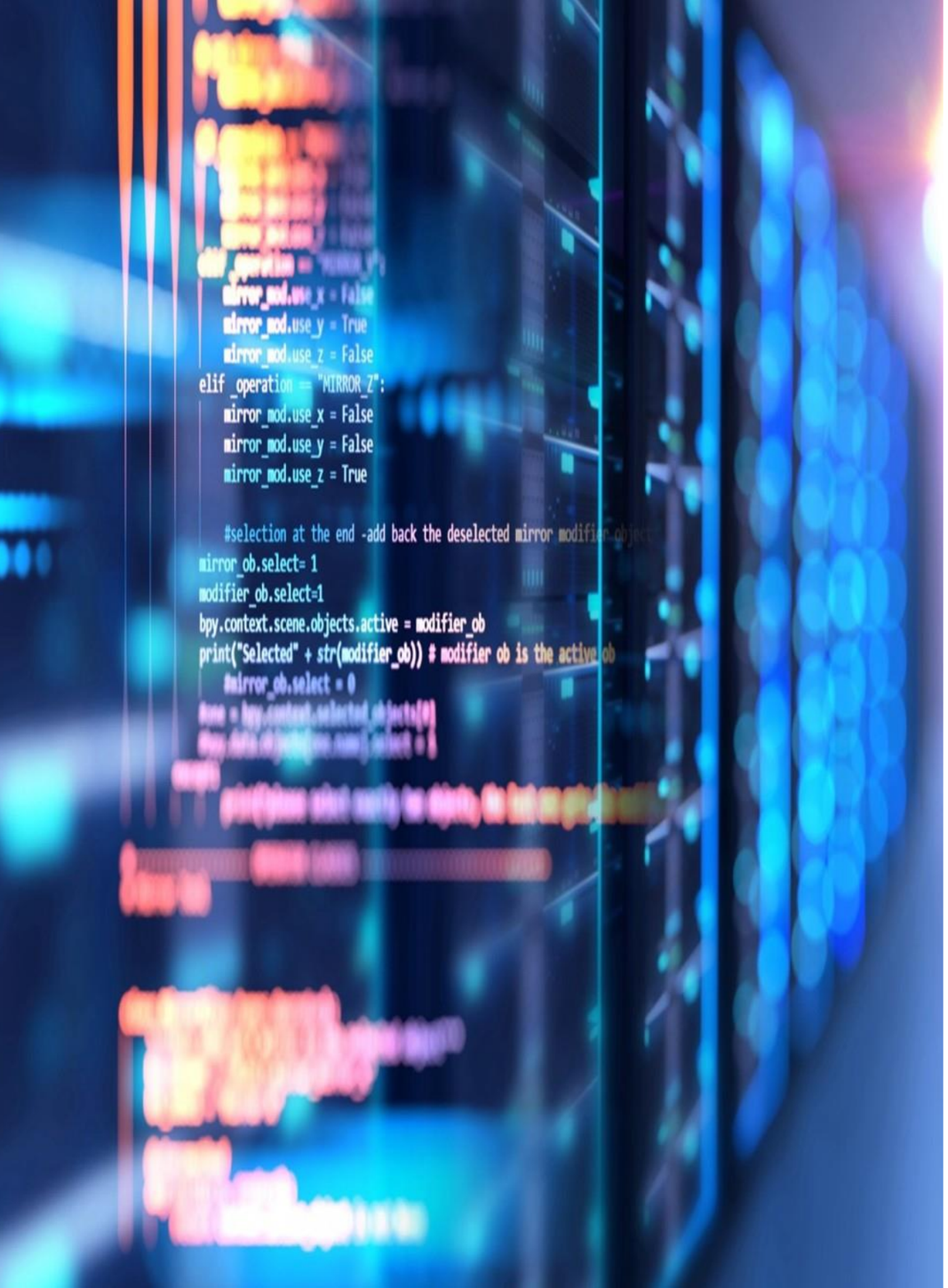
Factory-default passwords on inverters, gateways, and HMIs remain unchanged across thousands of deployed assets

Internet-Exposed Interfaces

SCADA and monitoring dashboards reachable via public IP, often indexed by Shodan or Censys

Cloud Dashboard Risk

Third-party cloud portals for O&M create credential exposure and API attack vectors outside the plant perimeter



Cyber Security and Resilience Bill

Expanded scope Includes digital service providers, managed service providers data centres and critical suppliers

Stricter Incident Reporting Initial report within 24 hours, more detailed report after 72 hours

Supply Chain Security Regulators will be able designate critical suppliers who will be subject to mandatory cyber requirements

Increased Penalties Up to £17 million, or 4% of worldwide turnover for more series breaches

Up to £10 million, or 2% of worldwide turnover for less serious breaches.

KEY ACTIONS TO IMPROVE READINESS & RESPONSE

GOLDEN RULES FOR INDUSTRIAL CYBERSECURITY

- Establish a Comprehensive Cybersecurity Baseline
- Adopt a Holistic Defense Strategy
- Recognize and Address Human Factors
- Implement & Regularly Update Security Policies
- Conduct Regular Assessments & Simulations
- Stay Informed About Emerging Threats
- Foster Collaborative Defense Efforts

IMMEDIATE ACTIONS

Start with initiating the risk assessment to identify your highest risks. In parallel start with initial technical activities

Stop the Attack Surface

Enforce MFA on ALL Remote Access

No exceptions. Remote access without MFA is an open door for credential-based attacks.

Build a Complete OT Asset Inventory

You cannot protect what you cannot see. Enumerate every device, every connection.

Segment IT and OT Networks

Flat networks allow attackers to pivot freely. Segmentation contains the blast radius.

Remove Default and Shared Credentials

Default passwords and shared accounts are among the most commonly exploited vulnerabilities in OT.

Rapid Risk Assessment Track

Perform a Rapid Risk Assessment

Map your exposure before you invest. Know your most critical assets and their current protection level.

Identify Highest-Risk Access Points

Remote connections, vendor jump servers, and IT/OT bridges are prime targets. Find them first.

Prioritise Critical Vulnerabilities

Not all CVEs are equal. Focus on what is reachable, exploitable, and impactful today.

Focus on What Can Be Exploited Today

Attackers move fast. Your remediation priority must match their exploitation timeline.

OFFSHORE WIND CRISIS EXERCISE

Logistics

- Full day Live simulation
- December 2025
- Utrecht, Netherlands

Facilitators

- BV Cyber
- TKI Offshore Energy
- Ministry of Economic Affairs
- Dutch Intelligence Services
- NCSC

Scenario

- Nation State Attack
- Insider OEM compromise
- Offshore Wind Sector in NL Disrupted

Participants

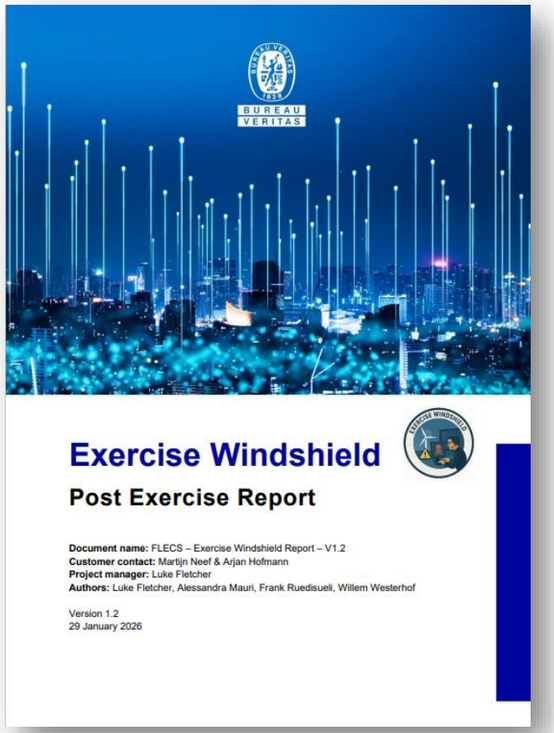
- Original Equipment Manufacturers
- Windfarm Operators
- Energy Distributors

Luke Fletcher

Principal Cyber Crisis Management Consultant luke.fletcher@bureauveritas.com

POST EXERCISE LESSONS LEARNED

Scenario Workshops



Crisis Response Shared Planning

Sector Crisis Management Framework

IOC and Sector Wide Situational Awareness

Luke Fletcher

Principal Cyber Crisis Management Consultant luke.fletcher@bureauveritas.com

Future Outlook – What's Next in Cybersecurity?

01

AI-Powered Cyberattacks

Attackers will use AI for automated phishing, deepfake scams, and adaptive malware.

02

Quantum Computing & Encryption Risks

Quantum advancements could break current encryption, requiring post-quantum cryptography.

03

Cyber Warfare & Geopolitical Threats

Nation-state actors will increasingly target critical infrastructure and supply chains.

04

Expanding Attack Surface

The rise of IoT, smart cities, and remote work increases security vulnerabilities.

Shaping a World of Trust