Current performance: Cyber resilience

WESTERN POWER DISTRIBUTION
Serving the Midlands, South West and Wales

Cyber Security for: 1) **Traditional Information Technology (IT)** – e.g. PCs, applications etc.
2) **Operational Technology (OT)** e.g. comms between systems and physical assets

- **Network and Information Systems (NIS) legislation** came into UK law in 2018
  - *Requires WPD to demonstrate active cyber security risk management, report incidents that disrupt energy supply and take action to rectify those incidents. We have:*

Implemented holistic risk management framework and incident response process for IT and OT

Segregated our Critical National Infrastructure systems from our corporate network

Increased logging and monitoring capabilities to capture possible cyber events

Increased threat intelligence sources giving greater insight and fast response to threats and risks

Expanded our program for managing system updates maintaining a high level of system security

- **7,500** desktops, laptops, servers and smart devices to secure
- We traditionally take data from **1,800** primary substation sites
- In future, likely to take data from c.**200,000** distribution sites
- **122,000** malicious e-mails blocked a month

Playback and draft outputs

WESTERN POWER DISTRIBUTION
Serving the Midlands, South West and Wales

Business IT Security & Cyber resilience

What we heard from you:

ENHANCING CYBER SECURITY

- Network security and resilience are becoming more important as electricity networks are increasingly **critical infrastructure for society**
- WPD should be **100% resistant** to cyber attacks
- **Collaboration between companies** should be encouraged to share best practice and stay ahead of hacking technology

DISASTER RECOVERY AND FUTURE PROOFING

- The impacts of cyber threats could be severe for customers. Therefore **disaster recovery** should be a high priority
- WPD's resilience planning should cover **anticipated changes in future network demand** and structure – e.g. greater reliance on electricity in heat and transport

And so the outputs we are proposing:

Enhance our cyber security systems to protect critical systems from unauthorised access leading to data or network disruption

Continually assess emerging threats and install next generation anti-virus and security systems to mitigate against these risks in line with National Cyber Security Centre guidelines

Enhance the resilience of our IT network by upgrading our disaster recovery capability

Development and implementation of new systems, technologies and applications that are capable of supporting the future network