WESTERN POWER DISTRIBUTION

Serving the Midlands, South West and Wales

Cyber Security Strategy

July 2021

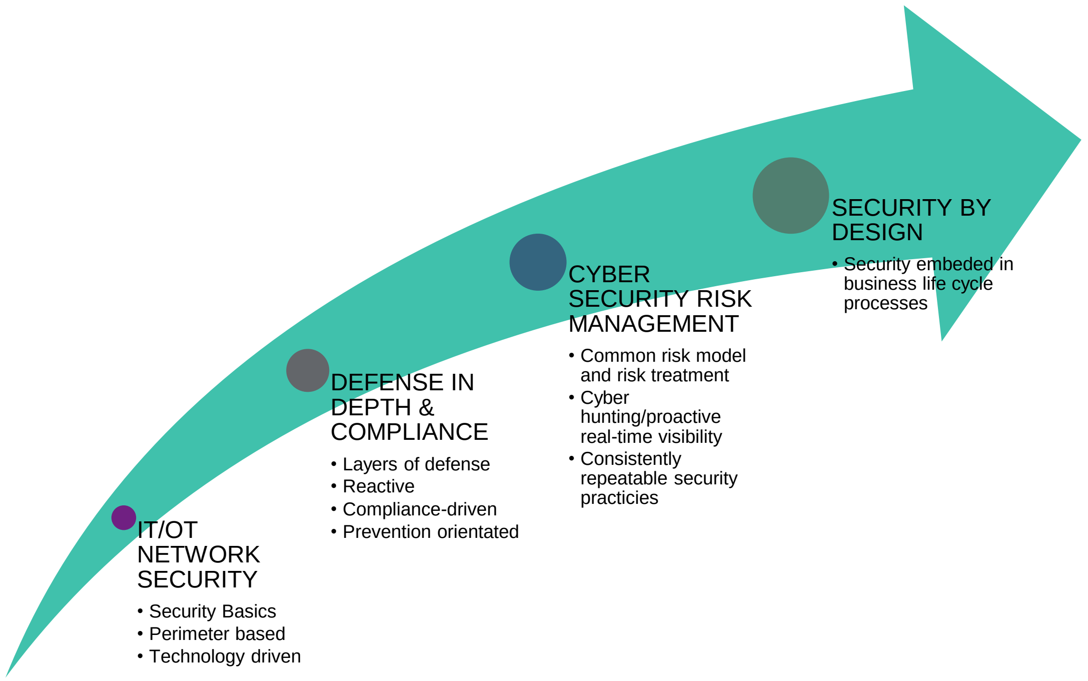
westernpower.co.uk

Contents

Cyber Security Strategy – Overview

In order to maintain reliable services to our customers, our goal is to protect and defend our IT and OT digital assets from the threat/disruption of cyber-events, but should they occur, be able to quickly respond to minimize the impact of any disruption.

This will be achieved by developing and maturing our cyber security practices as shown below:



IT/OT NETWORK SECURITY
• Security Basics
• Perimeter based
• Technology driven
DEFENSE IN DEPTH & COMPLIANCE
• Layers of defense
• Reactive
• Compliance-driven
• Prevention orientated
CYBER SECURITY RISK MANAGEMENT
• Common risk model and risk treatment
• Cyber hunting/proactive real-time visibility
• Consistently repeatable security practicies
SECURITY BY DESIGN
• Security embeded in business life cycle processes

Figure 1- Cyber Security Maturity Model

Key Principles

Our key cyber security principles are aligned to the Cyber Assessment Framework (CAF) as defined in the Network Information System (NIS) directive, with appropriate security controls implemented and applied as required. This is further underpinned by our risk management ethos of applying appropriate cyber security controls to IT/OT systems based upon risk and business criticality.

Our 5 key principles and cyber commitments are as follows:

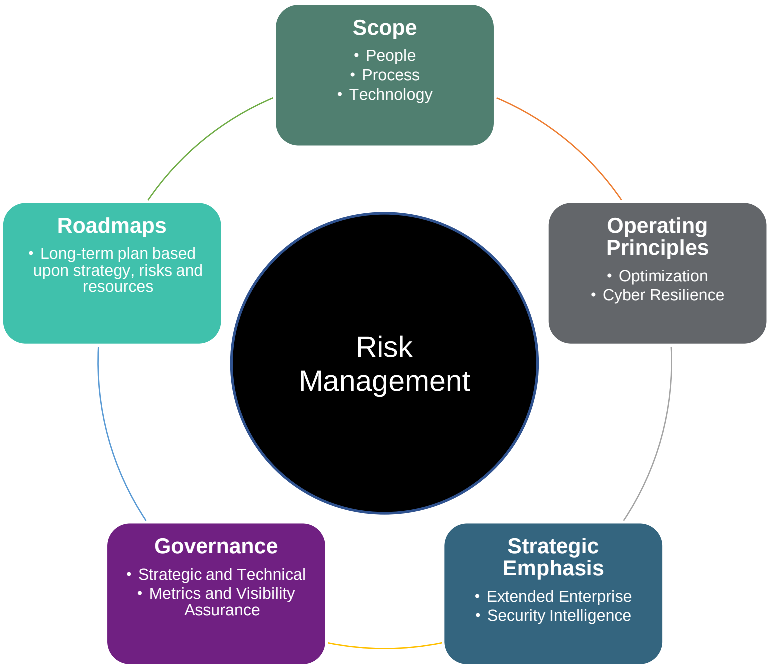


Figure 2 - 5 Key Cyber Security Principles

Scope

People

- Continuously improve senior leadership team’s cyber acumen.
- Work with staff to raise cyber security awareness through planned training and education programmes.
- Access Controls - Incremental tightening of privileged access for the individual, with an ethos of least privilege access.
- Cyber Technical Prowess – Advanced lab based training and workshops to ensure cyber analysts are trained on the most important and emerging technologies and approaches in cybersecurity.
- A centralised Cyber Security team will provide governance, controls and common standards for Cyber Security across the business.

Process

- Further define and develop IT security policies.
- Embed cyber security into WPD’s business processes and supply chain activities.
- Define security policies to detail the standards and controls to be applied to OT services.

Technology

- Ensure that new IT and OT Cyber technologies are fit for purpose and operate with exiting systems and technologies without being service affecting.
- Integrated, built-in security architecture will be utilised where possible.

Operating Principles

Optimisation

- Analyse capabilities of current cyber security technology investments to establish where already implemented solutions can be further utilised.
- Dedicated, skilled cyber security resource will be provided in-house supplemented with specialist expert 3rd party resource as and where required.

Cyber Resiliency

- Continued emphasis on business processes in support of cyber events, incident response, and recovery.
- Evolve threat detection, incident response, and proactive cyber hunting capability.

Strategic Emphasis

Extended Enterprise

- Reduction of the technology debt and a move to IT modernisation.
- Increased emphasis on ICS/OT security areas, in particular to gain cyber security visibility of OT assets, network traffic and vulnerabilities.
- Standardisation of scalable technology solutions for both IT and OT to improve security and gain economies of scale.
- Continued emphasis on data security and support to the business in relation to its Digitalisation strategy.

Security Intelligence

- Advance cyber threat intelligence capabilities, through automation and the collaboration with 3rd party security specialists.
- Further collaboration between physical and cyber security.

Governance

Strategic and Technical

- Extend cyber governance over time beyond strategic to practical technical governance that supports the cyber strategy and WPD's strategic imperatives.

Metrics and Visibility

- Evolve and mature cybersecurity risk metrics and continue to assess security posture against industry recognised benchmarking standards.
- Improve coverage of real-time asset visibility for on-going risk assessment and controls verification.

Assurance

- Evolve 3rd Line roles and activities to improve overall risk management.
- Work with internal audit and external assessors to further improve existing cyber security practices and controls within WPD.

WESTERN POWER DISTRIBUTION

Serving the Midlands, South West and Wales

Western Power Distribution (East Midlands) plc, No2366923
Western Power Distribution (West Midlands) plc, No3600574
Western Power Distribution (South West) plc, No2366894
Western Power Distribution (South Wales) plc, No2366985

Registered in England and Wales
Registered Office: Avonbank, Feeder Road, Bristol BS2 0TB

www.westernpower.co.uk

@wpduk