Cybersecurity Risk Management & Business Continuity – Offshore Wind Farm Case Study

Scenario Overview
ABC Enterprises, a mid-sized energy company valued at $10 million AUD, has recently transitioned its operations from land-based wind energy generation to an offshore (sea-based) wind farm. The transition was driven by opportunities to harness stronger and more consistent wind resources offshore. However, this move was executed without sufficient cybersecurity controls in place, exposing the organisation to significant operational and financial risks. **Cybersecurity Risks**
The new offshore environment faces a heightened attack surface, including threats such as ransomware, malware, distributed denial-of-service (DDoS) attacks, and TCP/IP hijacking. These risks could disrupt energy production, impact stakeholder confidence, and lead to regulatory non-compliance. **Objectives of the Assessment**
As a cybersecurity consultant, my role was to:

- Research and analyse cyber-attacks on renewable energy companies globally (2012–2023).
- Provide case studies of real-world incidents, focusing on attack vectors, impacts, controls, and lessons learned.
- Identify and evaluate the top five risks relevant to ABC Enterprises' offshore operations.
- Recommend cybersecurity control strategies aligned with industry best practices and budget considerations.
- Develop a Business Continuity Plan (BCP) to ensure operational resilience in case of cyber incidents and data breaches.

Key Deliverables

- A research report with professional business formatting and Harvard-style references.
- Comparative risk tables analysing different cyber-attacks, their impacts, and mitigations.
- A Business Continuity Plan aligned with ISO 22301, detailing incident response and recovery procedures.

Framework Alignment
This project demonstrates alignment with globally recognised cybersecurity and risk management frameworks:

- ISO/IEC 27001: Information Security Management Systems.
- NIST Cybersecurity Framework (CSF).
- ACSC Essential Eight (Australian Cyber Security Centre).
- ISO 22301: Business Continuity Management Systems.
- ISO 31000: Risk Management principles and practices.

Skills Demonstrated

- Cybersecurity risk analysis and governance.
- Application of international standards and frameworks.
- Business continuity and incident response planning.
- Professional communication of technical and strategic concepts.
- Research and evidence-based recommendations for critical infrastructure protection.