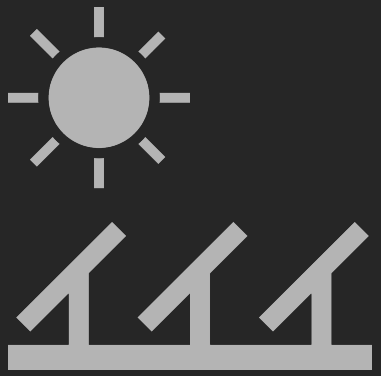

Information Security for Renewables
September, 2021

Kiowa
INFORMATION SECURITY

Kiowa approach

- Recognise that there are many aspects or layers to security, of which ‘software solutions’ is just one
- Reduce the attack surface; apply defence-in-depth
- Refer to
  - relevant specialised guidance e.g. NIST 800-82
  - general security frameworks e.g. ISO27001
  - alerts and threat updates (CISA, MITRE)
- Offer a range of potential vendor solutions; vendor-neutral stance

Kiowa
INFORMATION SECURITY

Cyber-threats

- Bad outcomes – ‘The damage’
  - Attacker accesses and disrupts ICS network and physical devices e.g. inverters, possibly causing economic loss and physical damage
  - Data breach and/or ransomware attack
  - Website attacks that disrupt online availability
  - Bank transfer fraud

- Attack vectors - ‘How it starts’
  - Phishing emails and messages
  - Malicious attachments and URLs
  - Insider threat – employees, contractors, suppliers with access
  - Supply chain attack
  - Attacks on VPN/remote access
  - Communications hijacking

Kiowa
INFORMATION SECURITY

Quick wins

- Physical security
- Housekeeping
  - Check configurations (everywhere, including cloud apps)
  - Patching
  - Block ports; turn off unused services
  - Use HTTPS, SFTP and other secure protocols
  - Lock down remote access

Kiowa
INFORMATION SECURITY

Personnel

- HR and contracts
  - Pre-employment screening
  - Reference in contracts to information security policy
  - Contractor agreements with e.g. O&M
  - NDA/confidentiality

- Training and education
  - Threat detection (e.g. phishing awareness)
  - Working securely
    - Password hygiene
    - Safe working from home/outside office
    - Acceptable use of devices
  - Incident and breach reporting

Kiowa
INFORMATION SECURITY

Supply chain security

- Check suppliers' current security arrangements
- Understand what access suppliers have and how it's controlled
- Check regarding sub-contractors of suppliers

- Software supply chain security
  - Mitigate 'dependency confusion' attacks
  - Disable arbitrary install commands by open-source packages
  - Enable MFA throughout the supply chain
  - Avoid exposure of sensitive information

Kiowa
INFORMATION SECURITY

Access and authentication

- Use MFA wherever possible
  - Risk based authentication
  - Tokens/smart cards
- Consider applying Zero Trust Network and Application Access
- Principle of least privilege – allow necessary access only
- Limit privileged access
- Review access rights and revoke when no longer required/contract ends

Kiowa
INFORMATION SECURITY

Insider threat protection

- Data Loss Prevention (DLP) to manage transmission of sensitive information
- Cloud Access Security to manage use of cloud applications and storage
- Configuration of applications to control and limit access to data
- Access control policies

- Employment and contractor contracts emphasize that failure to comply with information security requirements could lead to disciplinary and/or legal action

Kiowa
INFORMATION SECURITY

ICS security

- Information from asset developer regarding parts and vendors to check for vulnerabilities
- Use software to create and maintain an asset inventory
- ICS network monitoring
- Secure Remote Access for OT systems

Kiowa
INFORMATION SECURITY

Other digital solutions

- Data encrypted in transit and at rest
- Boundary protection; firewalls
- Network segmentation
- Backups

- Vulnerability scanning/penetration testing of networks and web applications

Kiowa
INFORMATION SECURITY

Cyber insurance

- ‘All risks’ policies pay out due to nearly any type of cyber attack, and cover most costs
- Cover:
  - Loss of income
  - Legal fees
  - IT costs and hardware replacement
  - Damage to assets
- Robust security policy reduces premium significantly

Kiowa
INFORMATION SECURITY

Business case for robust security; benefits include:

- ✓ Improved availability and reliability of the asset
- ✓ Improved employee morale and loyalty
- ✓ Increased investor confidence
- ✓ Reduced legal liabilities
- ✓ Happy regulator(s)
- ✓ Cheaper insurance with better coverage
- ✓ Becoming or indeed already a requirement of some third-parties e.g. off-takers

Kiowa
INFORMATION SECURITY

How Kiowa can help you:

- Advise on several aspects of implementation
  - HR; screening, contract wording
  - Security awareness training
  - Digital solutions including:
    - Access and authentication
    - Insider threat protection
    - ICS security
- Advise on implementation of ISO27001 framework and beyond
- Organise technical calls and POC’s with relevant vendors
- Deploy vendor solutions

Kiowa
INFORMATION SECURITY