Cybersecurity Checklist for Commercial EV Charger Installations

1. Physical Security

- Lock enclosures and disable or obscure USB/Ethernet debug ports.
- Use tamper-proof fasteners and enable tamper detection (if available).
- Secure physical mounting to prevent device theft.
- Enable RFID/card reader authentication if supported.

2. Network Security

- Place chargers on an isolated VLAN.
- Apply firewall rules to restrict outbound traffic to trusted domains/IPs.
- Disable public Wi-Fi or secure with WPA3 (or WPA2 minimum).
- Ensure all communications use TLS 1.2+ or VPN tunneling.

3. Firmware & Software

- Regularly update charger firmware; enable auto-updates if possible.
- Change all default usernames and passwords.
- Lock down or disable exposed APIs unless needed.
- Require 2FA for remote administrative access.

4. Logging & Monitoring

- Ensure charger logs are stored securely (Syslog, Cloud, etc.).
- Monitor for unusual usage patterns (time of use, session length).
- Forward logs to a central monitoring system or SIEM if applicable.

5. Supply Chain Integrity

- Choose reputable vendors with documented security practices.
- Request Software Bill of Materials (SBOM) from suppliers.
- Verify backend/cloud platform certifications (ISO 27001, SOC 2, etc.).