The top 8 cybersecurity items the operations department should be doing right now

1. **Governance**
   Assign OT security roles and responsibilities.
   Establish policies, procedures and guidelines

2. **Asset inventory**
   Know what you have, know how it is connected, know how (if) it is monitored

3. **Risk and Vulnerability management**
   Discover and address (mitigate/remediate) risks and vulnerabilities (patch, harden, update, etc.)

4. **Architecture and boundary defenses**
   Verify segmentation, remote access, traffic restriction, intrusion detection, functional isolation

5. **Log review and analysis**
   Verify all devices are monitored and review all alerts and logs for malicious/unauthorized activity

6. **Access controls**
   Verify default usernames and passwords have been changed and unused accounts removed

7. **Backup and recovery**
   Verify all assets and system assets have backups (or at least documented configurations)

8. **Secure configuration**
   Verify configurations per vendor guidance, disable unnecessary ports and services

EATON
Powering Business Worldwide

For those looking to develop their own robust cybersecurity program for their facility's networks, **Eaton's cybersecurity consulting services** can coach you every step of the way. Eaton also offers **Cybersecurity-as-a-Service,** ideal for those without the inhouse manpower and expertise to comply with industry standards and best practices.

Learn more at: **Eaton.sg/cybersecurity**