The top 7 cybersecurity items the operations department should be doing right now

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

2. Vulnerability management
   Discover and address (mitigate/remediate) vulnerabilities (patch, configuration, etc.)

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

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

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

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

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

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.com/CybersecurityServices