Cyber Vulnerability Management Considerations

Identify

- Determine the criticality and supportability of your IT and OT cyber assets.
- Understand the risk to operations of assets.
- Subscribe to government and vendor alerts.
- Maintain a Risk Register.

Protect

- Patch your assets.
- Reduce the attack surface.
- Maintain system and data backups.
- Maintain strong identity and access management.

Detect

- Scan assets for known vulnerabilities.
- Conduct red team exercises.
- Manage hardware and software life cycle planning and management.

Respond

- Evaluate the risk of each vulnerability.
- Implement risk-aligned approach and timeline necessary to remedy vulnerability.
- Invoke Incident Response Plan, when necessary.

Recover

- Establish/update (if needed) business continuity plan if vulnerable critical assets cannot be remediated.
- Test backup and recovery for critical assets.

References

1. National Institute of Standards and Technology (NIST) SP 800-40 Rev.4 (https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/draft)
2. Cybersecurity and Infrastructure Security Agency (CISA) Vulnerability Management FAQ (https://www.cisa.gov/uscert/cdm/capabilities/vuln)
3. Cyber Resilience Review Supplemental Resource Guide (https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-VM_0.pdf)
4. ISO 27001/27002 A.12.6.1 Management of Technical Vulnerabilities (a subscription is required to access this)

AGA
American Gas Association