Cisco recommends performing the following network resilience best practices, including updating hardware and software, securing administrative credentials, and continuously monitoring network environments.

**Credentials**
Choose complex passwords and community strings. Avoid default credentials. Use multi-factor authentication.

**Monitoring**
Secure monitoring and configuration traffic with encryption (SNMPv3, HTTPS, SSH).

**Restrict Access**
Restrict access and monitor credential systems (TACACS+, jump hosts).

**System Lifecycle**
Do not operate or deploy end-of-life or end-of-support hardware and software.

**Patch Management**
Keep software and infrastructure systems up to date.

**Change Management**
Proactively monitor the environment for unexpected changes and improve change management procedures.

**Infrastructure Logs**
Review syslog and AAA logs regularly for abnormal activities.

**Authorization**
Utilize AAA (Authentication, Authorization, & Accounting) best practices to prevent unauthorized configuration changes.

**Management Plane**
Protect the management plane with infrastructure ACLs (IACLs).

**Seek Assistance**
Seek assistance from Cisco TAC or PSIRT for security incidents involving Cisco products.

cisco.com/go/networkresilience