Cyber Threat Readiness Checklist: What to Do If Public Infrastructure Fails

This checklist is designed to help organizations prepare for disruptions to public cybersecurity infrastructure, including the CVE program, threat feeds, and vulnerability disclosure pipelines.

# 🔍 1. Asset Awareness

- [ ] Maintain a complete inventory of all hardware, software, and cloud services
- [ ] Tag critical assets that require continuous patching

# 🔁 2. Patch & Vulnerability Workflow Resilience

- [ ] Document how CVE data is used in your patching processes
- [ ] Identify alternative sources (vendor advisories, NVD, CISA Known Exploited Vulnerabilities Catalog)
- [ ] Test fallback workflows for at least one month each year

# 📡 3. Threat Intelligence Redundancy

- [ ] Subscribe to multiple threat intelligence feeds
- [ ] Use at least one aggregator with internal vulnerability mapping
- [ ] Monitor vendor-specific security bulletins for high-risk applications

# 🧾 4. Governance & Communication

- [ ] Include 'external threat intel dependency' in your risk register
- [ ] Assign responsibility for monitoring infrastructure funding disruptions
- [ ] Add a discussion item to your next board or leadership meeting

# 🧠 5. Partner & MSP Alignment

- [ ] Ask your IT provider how they monitor and respond to CVE disruptions
- [ ] Ensure your SLA includes continuity of patch intelligence in case of upstream issues

# ✅ Final Step

Set a reminder to review this checklist quarterly and after any major industry disruption.