



# Cyber Risk Vulnerability and Patch Management

## An approach for suppliers to protect data and systems

---

Cyber threats increasingly target information technology (IT) and operational technology (OT) systems by exploiting inconsistent patching practices. Effective vulnerability management helps reduce risk by identifying, assessing, prioritizing, and remediating known weaknesses in systems and software applications. This guide outlines the key principles, definitions, and actionable steps you can follow to build a robust vulnerability and patch management process.

### Defining the Terms

**Vulnerability Management** and **Patch Management** are two essential and complementary components of a robust cybersecurity and risk-mitigation strategy for IT, OT, and product environments.

**Vulnerability:** A flaw or weakness in software, hardware, or configuration that can be exploited by a threat actor to compromise confidentiality, integrity, and availability.

**Patch:** A software update issued by an authenticated source to fix vulnerabilities or bugs (errors in code) and improve functionality and/or security.

### Core Principles

- 1. Continuous monitoring:** Vulnerability management is not a one-time activity. New vulnerabilities emerge daily. Continuous, routine monitoring is essential.
- 2. Asset awareness:** Know what devices, applications, and systems you have [find tips in our [Asset Management Toolkit](#)]. You can't protect what you don't know exists.
- 3. Prioritized remediation:** Not all vulnerabilities are equal. The Common Vulnerability Scoring System (CVSS) is a standardized framework for assessing and communicating the severity of software vulnerabilities. Focus first on those that have the highest severity.
- 4. Patch proficiency:** Regularly apply vendor patches and updates, especially for internet-facing or business critical systems.
- 5. Accountability:** Assign clear ownership for patching and vulnerability resolution.
- 6. Balance:** Consider operational impact versus security need. Test patches before widespread deployment when possible.

## Understand Your Vulnerabilities

The best defense against a cyber attack is to understand your assets and know what vulnerabilities exist within your IT and OT estate. Identify failed security updates and unpatched vulnerabilities before attackers can exploit an opportunity. Use automated vulnerability scanning tools to continuously probe digital systems for weaknesses and opportunities that bad actors can exploit and use to infect organizations with viruses, ransomware, or other malicious programs. Having a Vulnerability Management Process for monitoring systems is an integral part of guarding against cyber attacks.

### The Vulnerability Management Process:

1. **Know what's on your network:** Create and maintain a list of hardware and software assets. (Known as asset management, this was explored in an earlier [Rolls-Royce toolkit](#)). Pay attention to legacy equipment, particularly obsolete products.
2. **Scan for vulnerabilities:** Use manual testing methods (e.g., penetration testing) or automated tools (e.g. Nessus) to scan internal and external systems. (OT scanning is often passive to avoid disruptions/downtime).
3. **Maintain awareness:** Keep informed about active threats in the greater business environment through threat intelligence reports and vendor advisories.
4. **Assess and prioritize:** Triage vulnerabilities. Use CVSS scores, reports of known exploits, system criticality, and exposure. Use a simple methodology to categorize vulnerabilities (critical, high, medium, low) to guide response timescales.
5. **Apply patches and fixes:** Apply critical or high-risk vulnerability patches and fixes within 14 days. Use centralized patch management tools where possible. For unsupported or legacy systems, isolate them and apply compensating controls (e.g., remove unapproved software or update unsupported software and protocols and fix configuration errors such as poor access control, security logging, or open ports).
6. **Back up and test before deployment:** Take backups of data before you start patching (in case you need to roll back your systems), and test on a staging platform or small number of devices before installing across your organization.
7. **Track and report progress:** Maintain a patching and remediation log. Track metrics such as:
  - a. Time to remediate critical vulnerabilities.
  - b. Percent of systems fully patched.
  - c. Repeat vulnerabilities.
8. **Assign responsibility:** Designate a person or team responsible for vulnerability management and provide basic training on identifying patch alerts and risks to your employees.


### Next Steps:

1. **Develop a policy, standards, and processes:** Define the frequency of scans, governance, operational roles and responsibilities, and patching response timelines.
2. **Start small:** Focus on key systems first (i.e., critical business applications, firewalls, servers, end-point devices).
3. **Leverage automation:** Use scanning tools to reduce manual effort.
4. **Review regularly:** Evaluate your vulnerability management and patching processes often and adjust based on evolving threats and business needs.
5. **Engage experts:** If resources are limited, consider procuring services from managed security service providers (MSSPs).

### Why are these steps critical for basic cybersecurity hygiene?

Attackers prey on vulnerabilities, yet you can't fix what you don't know. Asset inventories provide knowledge of devices and software across your IT and OT estate. Vulnerability management provides visibility into risks to assets, such as software flaws. Patching closes known paths to attackers.

For more information, contact:

 **Clare McBrearty**  
Rolls-Royce Supplier Cyber Security Lead  
[Clare.McBrearty@rolls-royce.com](mailto:Clare.McBrearty@rolls-royce.com)

If you would like a white label version of this toolkit to share with your suppliers, please request one from Clare.