5 Patch Risk Questions Every CIO and CISO Should Be Asking

AI is accelerating exploitation timelines. Can your operating model keep pace?

AI is making vulnerability discovery faster, exploit development easier and attack timelines shorter. Use these five questions to challenge assumptions, identify blind spots and spark discussion across IT, security and executive leadership teams.

ivanti

1

Where are we making decisions without full visibility into our environment?

Most organizations still have visibility gaps. The question is whether those blind spots are small enough to accept or large enough to create risk.

Ask your team:

- Where do we have the least confidence in our visibility today, and what would be the business impact if those assets were compromised?

2

Do we know our actual risk posture or just our compliance score?

Companies that tie remediation efforts to monthly patching cycles may be leaving known exploited vulnerabilities unaddressed for weeks, despite reporting high compliance scores.

Ask your team:

- Are our dashboards showing our true exposure window or our process completion rate?
- What exposure sources are we not counting, such as unmanaged assets, third-party software or shadow IT?

3

Has our organization defined what level of risk we're willing to accept, and are we measuring against it?

Every organization carries risk. The real question is whether that risk is being accepted intentionally or by default.

Ask your team:

- Where have we clearly defined our risk appetite, and where are teams making those decisions?
- Are our decisions driven by business impact, known exploitation activity, asset criticality or something else entirely?
- If two critical vulnerabilities appeared today, would leaders across IT, security and the business agree on which one should be addressed first?

4

Which parts of our response process would become obstacles during a major vulnerability event?

When exploit timelines shrink from weeks to days, every approval, review and handoff matters.

Ask your team:

- How long does it actually take us to remediate a known-exploited vulnerability?
- What changes would we need to make to reduce that timeline to 72 hours or less?

5

Which remediation decisions could be accelerated with AI and automation and which still require human judgment?

As exploit timelines shrink due to AI-accelerated attacks, organizations need scalable ways to continuously secure their environments and defend against emerging threats.

Ask your team:

- Where would automation create the greatest reduction in effort or response time?
- Where should we implement predefined policies and guardrails for AI and automation to help us move faster without sacrificing human oversight?

The organizations best prepared to face the AI-accelerated threat era will be the ones that can see risk clearly, make decisions quickly and respond with confidence as the pace of cyber risk continues to accelerate.

Understand the patch forward out of the Patch Apocalypse in our whitepaper: The Patch Apocalypse: Why Traditional Vulnerability Management is Breaking Under AI-Driven Discovery.

Click Here