Security metrics built for the boardroom may not show your current exposure



A Hacker News piece argues that many security metrics are assembled to be presented, not used, and so say little about what is happening in the environment week to week, a gap that matters as attackers speed up.

- The source says most security metrics are built to be shown, not used.
- Figures are often assembled shortly before a quarterly review and tidied for presentation.
- Such numbers reassure in a meeting but say little about the environment that week.
- The article ties the problem to attackers moving at AI speed.
- A linked item points to identity exposure and cross-domain privilege escalation as attack paths to map.

The article, published by The Hacker News, makes a simple observation about how security reporting works in practice. Most metrics, it says, are built to be shown rather than used. Between one quarterly review and the next status update, a set of numbers is pulled together, cleaned up and presented as a picture of a healthy program.

Why this matters

According to the source, those figures look reassuring in a room but tell almost no one what is actually happening across the environment in a given week. The headline links this gap to attackers moving at AI speed: if the picture is refreshed only before a meeting, it will lag behind the conditions it is meant to describe.

The excerpt we reviewed is short and does not set out the author's full method or any figures, so we limit ourselves to its central point.

Identity exposure as a related theme

A promoted item alongside the article refers to stories on how identity exposure opens active attack paths, and on mapping cross-domain privilege escalation to cut breach routes at key choke points. This is not the article's own analysis, but it indicates the kind of live, relationship-based view of risk the piece favours over periodic summaries.

For security and compliance leaders, the practical takeaway is to ask of every reported metric whether it is current, who acts on it, and what decision it changes. Numbers that exist only for the review cycle are a reporting product, not an operating tool.

What to do now

1. Review each metric in your board and committee reporting and record when its data was last refreshed.
2. Identify metrics that exist only for review cycles and replace or supplement them with near-real-time data where feasible.
3. Assign an owner and a decision to each key metric, so that a change in the number triggers an action.
4. Include identity exposure and privilege escalation paths in your exposure reporting.
5. Align the refreshed reporting with your existing NCA ECC and SAMA CSF control monitoring.