Is Board and Executive reliance on Cybersecurity Maturity Assessments misplaced?

The 2025 *Cybersecurity Board Reporting* project (www.cybersecurityboardreporting.com.au) identified the widespread use of maturity assessments to help Boards and Executives understand the organisation's cybersecurity posture. The **NIST Cybersecurity Framework (CSF)**, developed by the US National Institute of Standards and Technology, was found to be the most commonly adopted framework. It is supported by extensive guidance and tools that assist those conducting such assessments.

Maturity assessments provide a useful basis for organisations to benchmark their capabilities at a granular level against peers. They are also frequently used to determine target maturity levels and form part of broader cybersecurity strategies. For many organisations, therefore, maturity assessments have become a **core component of the cybersecurity information presented to Executives and Boards**.

However, our research also revealed a common shortcoming: many reports, including maturity assessments, give limited almostas they provided no visibility into **how much reliance can be placed on the results**. Directors often indicated that they derived comfort when reports were produced by third parties—yet even then, the level of validation can vary significantly.

Having worked on both the **consulting side** (delivering such reports) and the **organisational side** (consuming them), we observed clear limitations on the degree of reliance possible. Understanding *why* this is the case is essential.

Example: Assessing Patch Management Maturity

Consider the area of **patching**, which can be complex and full of exceptions—whether due to operational constraints or product limitations. Delayed patching remains a frequent source of cybersecurity breaches.

A maturity assessment of patch management may be performed in several different ways:

1. **Basic (Desktop) Assessment:**
   Conducted quickly in days through structured interviews or questionnaires with key stakeholders. It typically does not include detailed evidence gathering or verification of responses. A NIST maturity score is then assigned based solely on these discussions.

2. **Evidence-Based Desktop Assessment:**
   More comprehensive, often spanning several weeks. It includes collecting and reviewing supporting evidence such as patch logs or exception registers. A NIST maturity score is derived from both the discussions and the documentation reviewed.

3. **Validated (Testing-Based) Assessment:**
   The most rigorous and costly form. It involves technical testing to verify patch status, identify inconsistencies, or uncover unapproved exceptions. Although time-consuming, this approach provides the highest level of assurance.

These three approaches, while all "maturity assessments," can produce markedly different results. Hence, it is critical that reports clearly describe the **scope, methodology, and extent of validation** undertaken. Unfortunately, most reports we reviewed lacked this essential context.

Why This Matters

Unlike financial reporting, which benefits from centuries of refinement and well-established audit standards, **cybersecurity risk practices are still maturing**. Financial statements accompanied by an audit report communicate an understood level of assurance and rigour. No equivalent standards yet exist for cybersecurity reporting.
Our review of available frameworks and guidance across multiple jurisdictions revealed only limited direction concerning **cybersecurity reporting to Boards**.

To address this gap, Boards and Executives must consciously evaluate the **limitations** of cybersecurity reports they receive. When the degree of verification is unclear, further inquiry is warranted.

Questions Boards Should Ask

To establish the reliability of any cybersecurity maturity assessment or related other reports on which Directors are relying, Boards and Executives should seek clarity on:

1. **What was the scope of the review?**
2. **Who performed the work?**
3. **What level of testing or validation was undertaken?**
4. **What level of assurance was provided with the report?**

These questions can help determine whether additional information or assurance is needed.
Ultimately, Executives and Boards require sufficient context to judge **how much reliance** they can place on a maturity assessment, or report—particularly when it informs strategic direction or future investment in cybersecurity capability.