[redacted] [redacted]
Subject: Comments on CSF 2.0
Date: Thursday, May 4, 2023 7:48:13 PM

Thank you for the opportunity to review and comment on the preliminary discussion draft. My comments are on my blog at https://normanmarks.wordpress.com/2023/05/04/nist-and-cybersecurity-risk/.

The blog post concludes with:

1. ***Risk is the effect of uncertainty*** (in this case, the chance of a cyber breach) ***on enterprise objectives***. (Paraphrasing ISO 31000.) However, the NIST framework assesses and reports the risk to ***information assets***.
2. This creates a gap between the way business leaders talk and make decisions and the way cyber practitioners talk and provide information to decision-makers.
3. While the draft talks about understanding how cyber risk might affect the business and its performance, it does not explain whether risk will be measured by how it affects the likelihood of achieving enterprise objectives.
4. Cyber-related risk is just one of many operational sources of risk that need to be considered ***together*** when making a business decision.
5. Informed and intelligent decisions require the ability to compare and aggregate where necessary both upside and downside effects of uncertainty on the business, its performance, and its objectives.
6. It is impossible to make an informed and intelligent business decision when the choice is between investing to reduce the risk to information assets, mitigating safety risk, initiating a marketing plan to drive additional revenue, or accelerating the development of a new generation of products and services.

The answer, in my opinion (as explained with examples in Understanding the Business Risk that is Cyber: A guide for both business executives and InfoSec managers to bridge the gap) is to assess everything, both upside and downsides, in terms of ***how they might affect the achievement of enterprise objectives***.

This is what drives the leaders of the business, how their performance is measured, and it is in their language.

My recommendation to NIST is to ensure that this is the result of their risk assessment: not the risk to information assets, but the risk to affected enterprise objectives. How a breach would affect the likelihood of achieving them.

This approach enables the cyber practitioner to provide leaders and decision-makers with the information they need.

It can be compared and aggregated with other downside and upside risks.

Decisions about investing in cyber would no longer be made in a silo.

I am available to discuss the above.

Thanks
Norman

Norman D. Marks, CPA, CRMA
Author, Speaker, Thought Leader
OCEG Fellow, Honorary Fellow of the Institute of Risk Management

Join me online: My blog | Twitter | **LinkedIn**