From: Art Manion
Sent: Monday, January 22, 2018 7:51 PM
To: cyberframework <cyberframework@nist.gov>
Subject: coordinated vulnerability disclosure comments

Realizing that these comments are late, I'll provide them anyway in case they are useful or can still be considered.

I support the addition of coordinated vulnerability disclosure in RS.AN-5 and recommend that it remain in the CSF.

> RS.AN-5: Processes are established to receive, analyze and respond to
> vulnerabilities disclosed to the organization from internal and
> external sources (e.g. internal testing, security bulletins, or
> security researchers)
Regarding the Informative References:

> CIS CSC 4, 19
> COBIT 5 EDM03.02, DSS05.07
> NIST SP 800-53 Rev. 4 SI-5, PM-15

I have access to the CIS and SP 800-53 controls, I did not review the COBIT controls.

First, ISO 29147 should be cited. For example:

ISO/IEC 29147:2014 7, 9

(For reference, the titles of these clauses are "7 Receipt of vulnerability information" and "9 Dissemination of advisory")

ISO 30111 perhaps also:

ISO/IEC 30111:2013 6

("6 Policy and Organizational Framework for Vulnerability Handling Processes")

The 800-53 and CIS controls are somewhat relevant, but are designed for direct organizational defense. An organization should obtain vulnerability information, prioritize, and respond/publish. I'm mildly of the opinion to remove the CIS and 800-53 (and probably the COBIT) controls. Those control sets simply do not directly address coordinated vulnerability disclosure.

There is a long history of defensive controls focused on an organization better protecting itself. This is well and good. ISO 27000, CIS, SP 800-53 (and others?), COBIT (I assume), and the NIST CSF.

Coordinated vulnerability disclosure is about protecting others (customers, users/consumers of products and services the organization provides). This is a significantly different paradigm than protecting the organization. Thus, it has been difficult to find a good fit for coordinated vulnerability disclosure in the CSF (and in ISO 27000, and I don't believe it exists in COBIT or CSC or other NIST guidance). This is not a criticism of the CSF, just an observation that "protect critical infrastructure" and "protect all USG infrastructure" are not sufficient -- organizations need to "protect others from vulnerabilities in products/services provided by the organization."

Organizations are responsible not only for their own security, but the security of others. It is critical to teach and reinforce this way of thinking, which is why RS.AN-5 is an important addition to the CSF.

Regards,

- Art

Art Manion
Vulnerability Analysis Technical Manager CERT Coordination Center