NIST CYBERSECURITY FRAMEWORK 2.0 COMMENT

by Willard Grondski, BS, ITIL, A+, Network+, Security+

August 14, 2023

1. Govern
2. Identify
3. Protect
4. Detect
5. Respond
6. Recover
7. Report

I submit the addition of # 7 "Report" as a suggestion for inclusion to the NIST Cybersecurity Framework 2.0. The numbers speak for themselves:

1) According to the www.ic3.gov website, internet crime has risen from 351,937 complaints and $2.7 billion in losses in 2018 compared to 800,944 complaints and $10.3 billion in losses in 2022. These numbers represent a more than doubling the amount of complaints over only 4 years with nearly 4 times the losses in the same time period!

2) Unreported cyber crimes result in not only distorted, inaccurate, and unreliable statistics, but they also are a great cause for concern since there may be new vectors of attack, new malware, and new bad actor groups and all of this information would be of great value to law enforcement in the US and abroad. Time is a critical factor; the earlier that law enforcement receives this information, the sooner they can warn the public, alert the cybersecurity community, and track down these perpetrators.

The www.ic3.gov website states,

"Ransomware attacks impact individual users and businesses regardless of size or industry by causing service disruptions, financial loss, and in some cases, permanent loss of valuable data. While

ransomeware infection statistics are often highlighted in the media and by computer security companies, it has been challenging for the FBI to ascertain the true number of ransomeware victims as many infections go unreported to law enforcement."

This is why individual users and businesses need to be strongly encouraged to report any and all cyber crimes. Inclusion of the 7th step "Report" would go a long way towards accomplishing this.