METRICS? WHAT METRICS?

Finding the Missing Link to the NIST Cybersecurity Framework

The NIST Cybersecurity Framework (NIST CSF) is one of the cornerstones – and most popular features – of US government policy to strengthen our nation's cybersecurity. The hottest topic at the recent NIST workshop aimed at updating and refining the CSF was the development of metrics.

Many experts believe that for the CSF to properly evolve, or possibly even for it survive, the contentious metrics issue must be resolved. The key to moving forward on this issue is a better definition of what needs to be done in this domain and what NIST's role ought to be.

Since the CSF was released in 2014, NIST has been generally resistant to the development of metrics, fearing they could lead to regulation based on the CSF. NIST has steadfastly, and with considerable industry support, maintained that the CSF was developed to be a voluntary model. If metrics based on CSF were to be developed, policy makers might misuse these measurements to develop mandates.

Since cybersecurity technology and threat vectors change far too quickly to keep up with mandated standards and practices, these mandates would be both inefficient and counter-productive, since they would divert scarce cybersecurity resources into compliance regimes, which might have little impact on actual security.

However, the constant and increasingly troubling drumbeat of cyberattacks combined with the inability to fulfill the requirements of Presidential Executive Order 13636—that the

CSF be cost effective and prioritized—has created irresistible pressure toward developing metrics for the CSF.

Even NIST, in its suggested 1.1 version of the CSF, included a detailed proposal for metrics development, albeit one that has received almost no support from the private sector, which has historically embraced the CSF.

Some have argued that the way around this problem is to develop metrics on NIST "use." However this is mostly a diversionary tactic with multiple problems. First of all, there is no consensus of what constitutes "use" of the CSF, so determining undefined usage rates is a substantively meaningless exercise. Second the goal is not CSF usage, but security. To link NIST usage automatically to improved security is an unproven premise belied by the increased successful attacks. We need to show not just the CSF is used but that it is effective—indeed cost-effective—to fulfill the dictates of the Executive Order and actually improve our nation's security.

The reality, I believe, is that use of the CSF is effective, but exactly what elements of the CSF are effective and the degree of effectiveness likely changes from organization to organization based a number of variables such as size, sector, culture and business plan.

In a new e-book, An Executives Guide to Cyber Risk Economics, Jack Jones of the FAIR Institute points out that none of the commonly used measurement methods tell us what we really need to know which is how much risk exists and how that will change if this or that is done. What we need is an "explicit" risk measurement that measures risk in terms of event likelihood

and impact done in a quantitatively computational model that generates probabilistic and economically focused results.

The next step in the evolution of the NIST CSF shouldn't be to identify which elements of the CSF are cost-effective in general, but to develop an analytical tool that will enable individual entities to assess their unique threats on a monetized basis and assess which elements of the CSF will be most cost-effective in addressing them.

The development and validation of this tool is the missing link between the unique cyber threats organizations face, the large menu of standards and practices contained in the CSF, and the need to address these threats in a cost-efficient, and thus sustainable, basis.

The private sector is making progress in developing these tools on an open source basis. One such example is the FAIR model. ISA and the FAIR Institute have jointly appealed to NIST and DHS to support the further development, propagation, and testing of this open source tool as the focal point of NIST's next steps in resolving the metrics issue.

Supporting this proposal is a win-win-win. If the industry-government partnership can come together and not only define the "what" (the NIST CSF), but assist in defining "how" the CSF can be most effectively used, there will almost certainly be greater usage.

If we can demonstrate the cost-effectiveness of the CSF on an individualized entity basis, not only will there be no need for regulation (because entities will naturally adopt measures they know are cost-effective) but this individualized demonstration

will further demonstrate why one-size-fits-all mandates are inappropriate for cybersecurity.

Finally, and most significantly, by demonstrating a cost-effective process to enhance cybersecurity for the first time moves us firmly away from a 20th century compliance model and drives us toward a model based on actual security instead of compliance.

Written by Larry Clinton, ISA President and CEO