Steven J. Ross, CISA, CISSP, MBCP, is executive principal of Risk Masters Inc. Ross has been writing one of the *Journal*'s most popular columns since 1998. He can be reached at *stross@riskmastersinc.com.*

Frameworkers of the World, Unite 2

Every now and again, I like to take a poke at standards, just to see what makes them work.[1] Under consideration here is the cybersecurity framework published by the US National Institute of Standards and Technology[2] early in 2014. This document is no longer breaking news; I am more interested in how organizations might comply with it now that it is well known.

I can understand compliance with laws, regulations and even standards. But a framework? It would be easy to say that compliance with a framework is a *non sequitur,* but that would not account for the perception of the document since its publication.[3] In the absence of a true standard, it is being treated as one by many of the organizations with which I am familiar.

Of course, evaluation of a framework as though it were a standard can lead to some very unfair criticism. But then, explicit standards come in for their share of contumely as well. I want to make clear that I think the NIST framework is an excellent beginning of what must be a long process of applying standards to the defense against cyberattacks. I should add that as a publication of the US government, it formally applies only to US government agencies. However, as was made clear in NIST's recent *Update on the Cybersecurity Framework,*[4] it is being applied by a wide swath of the private sector, and international alignment is a major objective of these organizations.[5]

STRUCTURE OF THE FRAMEWORK

The framework is organized in a way that only a bureaucrat could love. There is the framework core, which is composed of functions, which begat categories and subcategories and then information references. Following the framework core, there are framework implementation tiers and a description of framework profiles. Of all these, only the subcategories provide any direction whatsoever toward cybersecurity.

The implementation tiers describe different levels of what can only be termed compliance with the framework, ranging from partial to adaptive. Even NIST admits that the tiers are "the least-used part of the Framework," ascribing this to "their enterprise-level scope."[6] I say it is because there is no purpose to being just a little compliant with a standard (oops, a framework) that is supposed to lead to security, so organizations are only paying attention to the adaptive tier.

The profiles are a way of describing the as-is and will-be states of compliance with the framework. The terms used are "current profile" and "target profile." I find this terminology confusing, and NIST accepts that it is "clear that there remains some confusion over terminology that should be addressed in future efforts."[7]

REFERENCES TO OTHER STANDARDS

For each of the subcategories, there are references given to other standards and frameworks on which the framework is built. These include other NIST standards, ISO 27001 and ISACA's COBIT®.[8] The cross-references are both strengths and weaknesses of the framework.

They are a strength in that they place the framework specifically, and cybersecurity more generally, within the context of information security as it has been known and practiced for many years. With all of these other standards and frameworks, it would seem that there is no need for the Cybersecurity Framework at all...that all an organization needs to do is comply with all the referenced standards and—voila!—cybersecurity will take care of itself. Of course, if a corporation or government agency adhered to every listed standard in detail, plus others not mentioned,[9] they would be so busy complying that they would not have time for information technology and, therefore, would not be at risk. Okay, a bit of an exaggeration, but even if they did comply with all those standards, would they have achieved *cyber*security?

FORUM

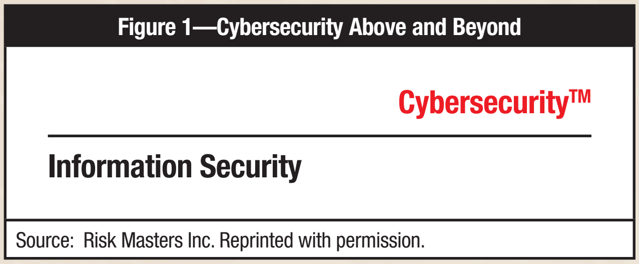
Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and choose the Comments tab to share your thoughts.

Go directly to the article:

That question, to my mind, points to a weakness of the framework. There is no doubt in my mind that effective cybersecurity rests on a foundation of information security, just as effective information security is built upon a system of internal control. But the need for cybersecurity derives from a substantively different threat—that of organized attackers targeting the systems and information of specific organizations. For that reason, cybersecurity is above and beyond information security (**figure 1**).[10]

Figure 1—Cybersecurity Above and Beyond



Source: Risk Masters Inc. Reprinted with permission.

Compliance with the NIST Cybersecurity Framework requires an organization to put in place a series of measures specifically designed to address *cyber*threats. I take issue with the framework in that in many of its functions, it conflates information security and cybersecurity.

Information security is business-driven. The differential requirement for security in any organization is based on risk management, an industry-by-industry, business-by-business appreciation of the potential for abuse of information resources. Information security results in prudent investment in safeguards and countermeasures. Cybersecurity is threat-driven, the menace being well-financed, expert, patient criminals, terrorists and governments. All of an organization's information assets are at risk, because their interconnectedness exposes all of them to a failure of their most vulnerable elements. As a result of not differentiating the two, the majority of subcategories in the framework are not directly focused on the issue of cybersecurity. Of the 98 subcategories in the framework, only 32 of them directly address cybersecurity (by my count).

“Effective cybersecurity rests on a foundation of information security, just as effective information security is built upon a system of internal control.”

Enjoying this article?

- Read *Implementing the NIST Cybersecurity Framework*.

www.isaca.org/ US-cyber-implementation

- Learn more about, discuss and collaborate on frameworks and cybersecurity in the Knowledge Center.

www.isaca.org/knowledgecenter

THE 20-YEAR RULE

I come to that conclusion by applying what I call the 20-year Rule. If there was a security measure I was using 20 years ago, it was not a cybersecurity safeguard, because I was not worried about cyberattacks that long ago. So, for example, in the Identify function, Asset Management category of the Cybersecurity Framework, there are six subcategories:

1. Physical devices and systems within the organization are inventoried.
2. Software platforms and applications within the organization are inventoried.
3. Organizational communication and data flows are mapped.
4. External information systems are cataloged.
5. Resources (e.g., hardware, devices, data, software) are prioritized based on their classification, criticality and business value.
6. Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.

All but the last subcategory fall under the 20-year Rule. That is, only the sixth one addresses a cybersecurity-specific control. Again, it is not that the first five are unimportant; it is just that they are not specific to the threats of cyberattacks, cybercrimes, cybertheft, etc.

But lookie here what I found lurking in the middle of a perfectly nice framework: The 32 subcategories that are cybersecurity-specific constitute a *standard*. Or perhaps it would be better to say they constitute the beginnings of a standard, since they do not have much depth. For instance, a statement that "incident alert thresholds are established" cries out for answers to what are appropriate thresholds and what should happen if they are surpassed.

NIST states that "the framework developers' intention [was] to encourage alignment among standards already in use." It is to be hoped that new standards will arise that address the open questions raised in this important step supporting broad appreciation of cybersecurity.

ENDNOTES

[1] An article of this same name, minus the 2, appeared in this space in volume 6, 2004. And once again, thanks go to the late William Safire of *The New York Times* for this play on words.

[2] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, USA, 2013. I will refer to it simply as "the framework" here, although I have seen it referred to as NCsF. A search on "ncsf" has convinced me to stay away from that acronym.

[3] See, for example, PivotPoint Security, "Does ISO 27001 Certification Make You NIST Cybersecurity Framework Compliant?" Information Security Blog, *www.pivotpointsecurity.com/risky-business/iso-27001-nist-cybersecurity-framework-compliance*, which directly addresses the issue of compliance.

[4] National Institute of Standards and Technology, *Update on the Cybersecurity Framework*, USA, 5 December 2014

[5] *Ibid.*, p. 5

[6] *Ibid.*, p. 2

[7] *Ibid.*, p. 3

[8] *Op cit*, NIST 2013, p. 35

[9] Such as Payment Card Industry Data Security Standard (PCI DSS), ISO 22301 or NFPA 1600

[10] The little representation of "above and beyond" in **figure 1** is a trademark of my consulting firm. I hereby grant irrevocable license to all readers of the *ISACA Journal* to reuse and reproduce it.