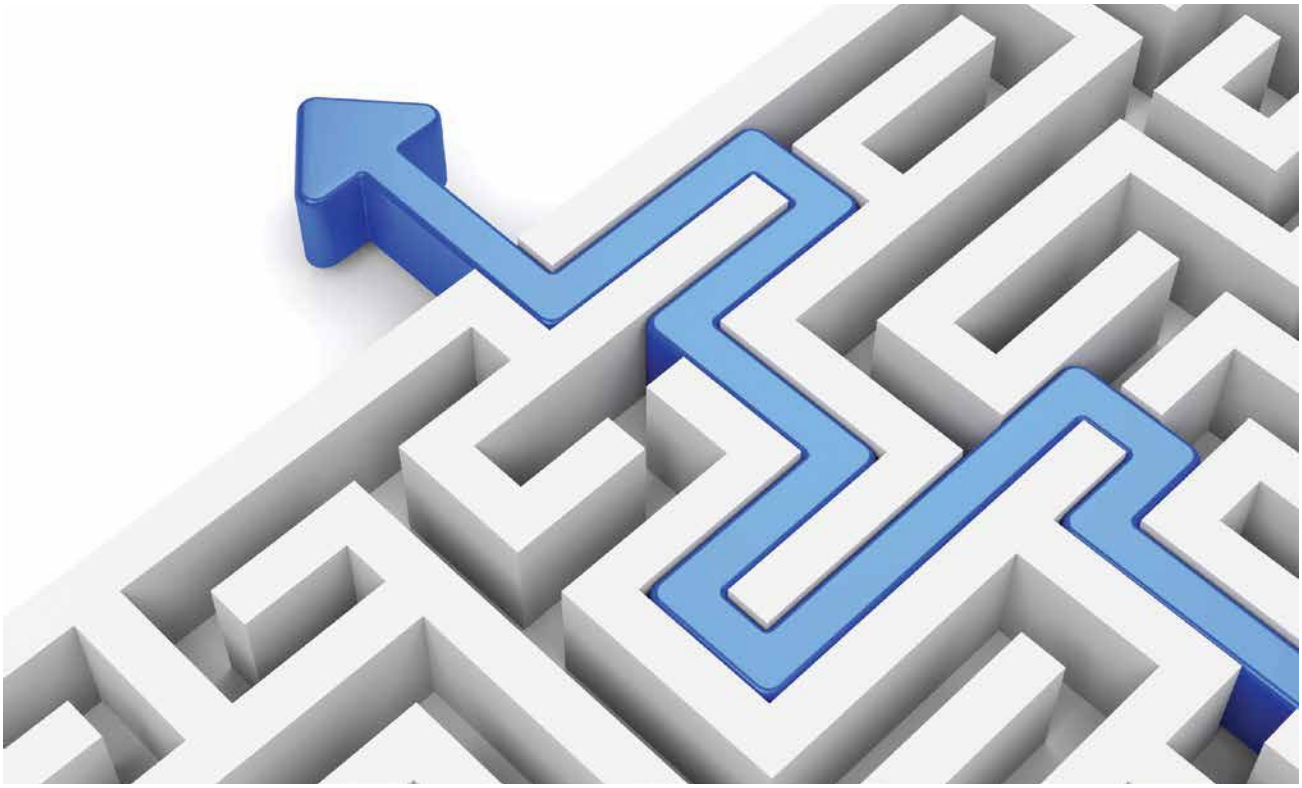
Benefiting from the **NIST Cybersecurity Framework**

Meg Scofield

"The Framework for Improving Critical Infrastructure Cybersecurity," which was published by the National Institute of Standards and Technology, acts as a Rosetta stone to help organizations translate and navigate among complex cybersecurity requirements. Its adaptability makes it applicable to a broad range of operating environments and potentially will make it the *de facto* industry standard.



Security breaches dominate the news. This past summer, a federal government computer hack compromised personal information belonging to 21.5 million individuals. In September 2014, Home Depot's credit card breach cost the company an estimated $62 million for damage control, like credit monitoring. Then, only a month later, network data bandits targeted Staples and stole more than 1.16 million credit cards.

For organizations, their leaders, and their customers, these incidents can mean professional – as well as personal – devastation. In addition to the significant expense incurred in just responding to a breach, there are financial and time losses resulting from ensuing lawsuits. Not so easily measured is the additional economic damage of the negative publicity.

Ever-increasing volumes of electronic information mean growing vulnerability to cyber-threats. Rather than assume the IT shop is handling the risks, a collaborative effort between IG and IT will best produce a strong information governance (IG) strategy and robust online protection.

The "Framework for Improving Critical Infrastructure Cybersecurity" (Framework), developed in 2014 by the National Institute of Standards and Technology (NIST). provides the common language collaborative parties need to talk about how organizations can keep online information safe.

(A free PDF of the Framework can be downloaded from *www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf*.)

A Path Through the Panic

In 2013, President Barack Obama issued Executive Order 13636 that directed NIST to work with government and private industry representatives to create guidelines to help critical infrastructure organizations keep their online platforms safe.

> ...an organization might begin by comparing existing information protection practices with those described in the document.

The order defines *critical infrastructure* as essential systems that, if impaired, would result in "a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Examples include public and private sector areas like utilities, health care, agriculture, chemical manufacturing, and water supply.

NIST, in developing the Framework, convened industry representatives and members of the public and asked what would be valuable for them. A year later, the answer became the Framework document, offering voluntary and technology-neutral precepts for information protection.

The Framework's Broad Relevance

Matt Barrett, NIST program manager for the Framework program, describes the financial services industry as a model that illustrates the Framework's relevance. The Framework has a role in ensuring the security of daily financial transactions like using an ATM machine, swiping a credit card, or making an online purchase.

"When critical infrastructure organizations win, we all win," Barrett says.

Not only critical infrastructure can benefit from using the Framework. NIST's website features use case studies from organizations as varied as Intel and the University of Pittsburgh. In addition, the Framework's reach has expanded to an international audience. A Japanese translation is available, and Italy produced cybersecurity guidance that incorporated the Framework's recommended activities.

NIST also encourages small companies to use the Framework, even if they think they are too insignificant to need to worry about cybersecurity.

Bruce deGrazia, J.D., CISSP, the University of Maryland's University College program chair and collegiate professor, cybersecurity, cautions, "It's what we in the field call *'Security by obscurity.'* The fact that we have a phrase for it indicates that it's not something you can hide behind."

On the other end of the spectrum, while U.S. federal government agencies may adopt Framework activities, they are not required to do so. Mandates and regulations for federal security come from the Federal Information Security Management Act (as amended), the White House Office of Management and Budget, and NIST's own standards and recommendations set forth in federal information processing standards and special publications.

Integrative Approach to Cybersecurity

As Barrett explains, with five functions, 22 categories, and 98 subcategories, the current Framework version 1.0 provides a standardized set of cybersecurity outcomes around which to convene and focus energy. Dialogue about online vulnerability can be internal to an organization, among organizations, or even between an organization and its customers.

In short, the Framework's guidelines can help comprehend and control risks to valuable online assets.

Executive consultant Ren Cahoon, of Reynolds Cahoon LLC (formerly CIO of the National Archives and Records Administration and senior advisor on electronic records to the archivist of the United States), explains the process as incorporating security with everything else that's going on in an organization. He encourages information professionals to use the Framework to become comfortable with cybersecurity – not necessarily to be an expert, but to gain a basic understanding of how cybersecurity contributes to overall governance of information.

Cahoon says, "Before the Framework, there was a lot published, people had a lot to say, but there was [nothing] comprehensive."

Technology Experts Not Required

While NIST is a technical organization, the Framework itself is designed for people who aren't technical experts.

Barrett describes the Framework as "an easy, breezy read," purposely different than a typical NIST publication that is hundreds of pages long and heavy on details. Instead, the Framework document is just under 40 pages long, 17 of which comprise the core body; appendices make up the rest.

Throughout 2015, NIST representatives offered workshops and attended conferences and other events across the country to help explain the Framework. The intent has been to publicize the Framework's components and to make sure that all participants, including those who may not be technologically adept, understand how implementing it can benefit their organizations.

"When it comes to total cybersecurity protection," deGrazia points

out, "the approach and the ability to address problems come from the management side."

Getting Started with the Framework

To use the NIST Framework, an organization might begin by comparing existing information protection practices with those described in the document.

Next, an organization might target areas of improvement. The Framework is not meant to replace successful activities, but to complement ongoing efforts and suggest new areas of focus. The analysis process is designed to be repeated at regular intervals.

The Framework's three sections daylight areas that need strengthening and serve as a guide to building areas that don't exist:

Core: This section outlines the basic functions – Identify, Protect, Detect, Respond, and Recover – that describe at a high level the continuous looping life cycle of cybersecurity activities. The five functions help prioritize resources and promote cybersecurity awareness.

Implementation Tiers: Four tiers (Partial, Risk Informed, Repeatable, and Adaptive) explain the range of risk management practices. Note that the tiers don't represent maturity levels. Moving from one tier to the next is tied to risk reduction and resources.

Profile: An organization can define goals and objectives via self-assessment of the "As-Is" state and the desired "To-Be" state.

Final segments include communicating cybersecurity expectations; adding or revising practices to tailor the guidelines to specific needs; and evaluating how personal information is collected and retained.

Cahoon suggests an organization think about how secure information and data can be managed in a holistic way. "Balance is important, the connection between security and access, between security and continuity of operations, and how retention is managed," he says.

He uses the analogy of building an incredible automobile to illustrate the concept. Bring together in a warehouse the best engineers and cars. From one model, engineers pull out the finest engine and from various other models the finest transmission and the best suspension, sound system, climate control, and so forth, putting them all in the middle of the warehouse. Cahoon explains, this isn't a car – only a pile of parts.

"If an organization is just implementing best practices all over the place, the parts don't fit together any better in an organization than they do in that warehouse with the pile of parts," Cahoon says. "It's a question of deciding what are the right practices for the organization in terms of risk, and integrating those practices in a way that really optimizes and

"The Framework for Improving Critical Infrastructure Cybersecurity"

Benefits	Section Features
Core: Reconciles and clarifies legislation, regulation, policy, and industry best practices	Reduces the time and expense of starting an information security program
Reduces risk within current information security programs by identifying areas for improvement	Core: Guides organization and management of an information security program
Increases efficiencies and reduces miscommunication within an organization and with stakeholders, such as customers, partners, suppliers, regulators, and auditors	Profile: Measures current state and expresses desired state Profile: Enables investment decisions to address gaps in current state Profile: Communicates cybersecurity requirements Tiers: Enables informed discussions of resources vs. risk

Source: National Institute of Standards and Technologies; adapted from a January 2015 NIST presentation, "From Framework to Action: Understanding the NIST Cybersecurity Framework"

tunes the organization to its highest performance."

Potential Benefits of Using the Framework

For Barrett, one of the Framework's advantages is its ability to navigate complex cybersecurity requirements and the operational landscape. "We have a dizzying number of things to help keep us secure," Barrett says. "The Framework acts as a Rosetta stone to translate amongst those."

The Framework's three sections daylight areas that need strengthening and serve as a guide to building areas that don't exist.

Because of the Framework's adaptability across a range of businesses and fields, deGrazia believes it will become the *de facto* industry standard, and, because of that, may help protect an organization from liability.

If someone tries to sue organizations that have implemented the Framework, deGrazia says the response could be, "Hey, we've got this Framework in place, we've done all the things that were recommended." It makes it easier for [organizations] to defend themselves in court against potential lawsuits."

Considerations for Using the Framework

While cybersecurity should be included as an integral part of how an organization functions, Cahoon recognizes it can also constrain an organization's productivity, even hinder information access.

"In some organizations, security casts a pall and makes doing things so complex and difficult that the costs of that security outpace the risk," Cahoon says. "Organizations mustn't let themselves be bullied by the paranoia around cybersecurity. Be sure cybersecurity is appropriately balanced with all the other important elements of the organization and efforts to accomplish its mission."

Because systems and platforms change frequently, specific technical prescriptions aren't part of the Framework.

Barrett says, "For those who are technically inclined, the Framework could be dissatisfying in that it's not meant to be a 'rubber meets the road' technical approach or methodology. That's on purpose."

Having presented the Framework to technical crowds, Barrett has had to regularly address the value proposition to them. His response?

"When we have things organized over top of that technical echelon," Barrett says, "it leads to efficiency, it leads to lack of confusion, it leads to lack of duplicate work, it leads to less interference from, for instance, evolving cybersecurity requirements, new legislation, new regulation. It enables technical folks to do their job with less drag."

On the other hand, deGrazia acknowledges that putting the approach into place isn't accomplished easily, quickly, or inexpensively.

"The Framework is not something that you can establish once and then walk away," deGrazia says. "It's going to have to be continually reviewed like any other policy would have to be reviewed, and continually updated. So you can't say, on Jan. 1st we've got the Framework in place, we've done everything, and we never have to worry again. I'm not sure that small- to medium-sized businesses recognize this."

For those organizations with limited resources, Cahoon adds another possible concern.

"From a small business perspective, there should be a 'Cybersecurity Framework Lite,' Cahoon says. "If I'm a small business, I'm going to do as much as is necessary to do, and no more. Not try to do so much that – number one – [a small business] can't function, and – number two – can't afford to implement it all. There needs to be something that's streamlined and simplified for the organization that can't afford a major cybersecurity function."

Future Directions

As the dynamic arena of cybersecurity shifts and changes, NIST encourages industry comments on the Framework.

In December 2015, NIST issued a request for information (RFI) asking for public feedback on a possible update to the Framework and what topics it might need to include. NIST also asked questions on future governance of the Framework, including what is the right balance between industry and government ownership of the Framework going forward to ensure maximum positive effect.

On April 6-7, 2016, NIST plans to host a workshop on the Framework in Gaithersburg, Maryland. The event will provide a forum to address topics of discussion from the RFI responses.

"NIST continues to be a convener relative to the Framework," Barrett says. "One of the things that offers the greatest level of value is that the Framework will evolve and improve over time."

That kind of open communication is vital – between NIST and Framework stakeholders, and between organizations' information professionals, business area representatives, legal experts, and senior leadership.

As material continues to be created and managed electronically, the Framework's developing guidelines will serve as an ally to any information owner determined to stay vigilant about managing risk. **END**

Meg Scofield *can be contacted at meg@twocoffeecups.com. See her bio on page 47.*