NIST Cybersecurity Framework Aims to Improve Critical Infrastructure

Yet another standard? No. What you'll see this month is a tool designed to bring together all the relevant cybersecurity standards and put them in an appropriate context—a framework—so you can manage cybersecurity risk more effectively. (And yes, managing that risk is everyone's business, regardless of job title.)

Steve Mustard

A year ago, on Feb. 12, 2013, President Obama issued Executive Order 13636, titled "Improving Critical Infrastructure Cybersecurity." The Executive Order instructed the National Institute of Standards and Technology (NIST) to develop a voluntary Cybersecurity Framework that would provide a "prioritized, flexible, repeatable, performance-based, and cost effective approach for assisting organizations responsible for critical infrastructure services to manage cybersecurity risk."

The definition of "critical infrastructure" in the Executive Order is: "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

As everyone working in the power industry understands, power generation and transmission assets are part of that critical infrastructure.

The State of Cybersecurity

Given the availability of a variety of standards for cybersecurity management, questions have been raised as to why an official Cybersecurity Framework is required. Furthermore, many of these standards have been in existence for many years, and a popular belief is that the requirements of these standards are being followed, so additional, similar standards will not help.

Unfortunately, the data show that even if current standards are being followed, they aren't providing sufficient protection. There are many publically available reports on cybersecurity attacks, and there has been a common theme throughout them for the past few years, exemplified by these statistics from Verizon's breach reports of 2012 and 2013:

- 97% avoidable with basic or intermediate security controls (2012)
- 92% discovered by a third party (2012)
- 20% of network intrusions involved manufacturing, transportation, and utilities (2013)
- 76% of network intrusions exploited weak or stolen credentials (2013)

The Verizon report (you can download it here: www.verizonenterprise.com/DBIR/2013/) used data from 19 global organizations, including law enforcement agencies, national incident-reporting agencies, research institutions, and private security firms.

The Repository of Industrial Security Incidents (RISI) produces an annual report that focuses specifically on industrial control systems (ICS), and these reports provide conclusions similar to those from Verizon. The 2013 RISI annual report stated that 33% of all ICS incidents were perpetrated using remote access.

The Verizon report from 2012 provides staggering temporal statistics relating to cybersecurity attacks. In 2012, 75% of attacks took just minutes to result in an organization being compromised; however, 54% of these compromises took months to be discovered (and, as noted, 92% of these discoveries were not by the organization itself). Even after this lengthy delay, in 17% of cases, it took months before restoration was achieved after the breach discovery, and in 38% of cases it took weeks.

The statistics from Verizon cover all sectors and industry types. Within industrial automation–oriented sectors the situation varies considerably. Many such organizations have mandatory cybersecurity standards—such as North American Electric Reliability Corp. Critical Infrastructure Protection (NERC CIP) in the power industry—and their cybersecurity management programs are good. However, many organizations that have a potentially high impact on the critical infrastructure (for instance, water and wastewater organizations) have a much lower degree of cybersecurity management adoption (Figure 1).

There are many reasons for this situation, and they include:

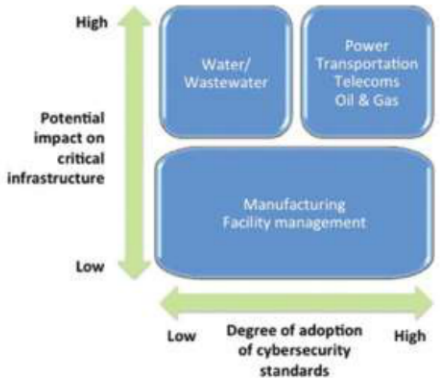
- Lack of awareness in organizations, in particular at the top of the organization.
- Misunderstanding the level of risk an organization has (for example, thinking "that only happens to other companies" or "this has never happened before").
- Inability to quantify the risk in likelihood or impact terms, resulting in inappropriate level of investment.
- Lack of adequate training in cybersecurity good practice, especially in regards to basic controls such as good password management, backups, and malware protection.

The purpose of the NIST Cybersecurity Framework is to help tackle some of these issues. The Cybersecurity Framework is not another standard. Instead, it is a high-level concept that brings together relevant standards and sets them in an appropriate context.

The Cybersecurity Framework Process

Following the Executive Order announcement in February 2013, NIST issued a request for information. More than 245 responses were received from asset owners, product vendors, and consultants from all

1. Cybersecurity standards adoption. The adoption of cybersecurity standards in the power industry may be higher than in some other sectors, but the impact of a compromised system is the highest. *Source: Steve Mustard*



industry sectors. NIST then arranged a series of five workshops from May through November last year at various locations around the country. At these workshops, typically 350 to 400 attendees representing asset owners, product vendors, and consultants debated various aspects of the Framework; between the workshops, NIST reworked the gathered information into new drafts.

The initial meetings focused heavily on information technology (IT) systems and the protection of data and information. Many attendees were unaware of the specific issues associated with ICS or operational technology (OT) systems where protection is required:

- Loss of system availability
- Process upsets leading to compromised process functionality, inferior product quality, lost production capacity, compromised process safety, or environmental releases
- Equipment damage
- Personal injury
- Violation of legal and regulatory requirements
- Risk to public health and confidence

The Automation Federation, along with a number of asset owners with OT dependencies, worked throughout the workshop process, raising awareness of these issues to ensure the Framework properly addresses them.

A draft of the Cybersecurity Framework was issued at the end of October 2013 for public comment. After a 45-day comment period, NIST will take the comments and produce a final version for issue in February 2014 (after this issue goes to press).

Once issued, the Cybersecurity Framework enters an ongoing maintenance and upkeep cycle to reflect changing circumstances and feedback from users.

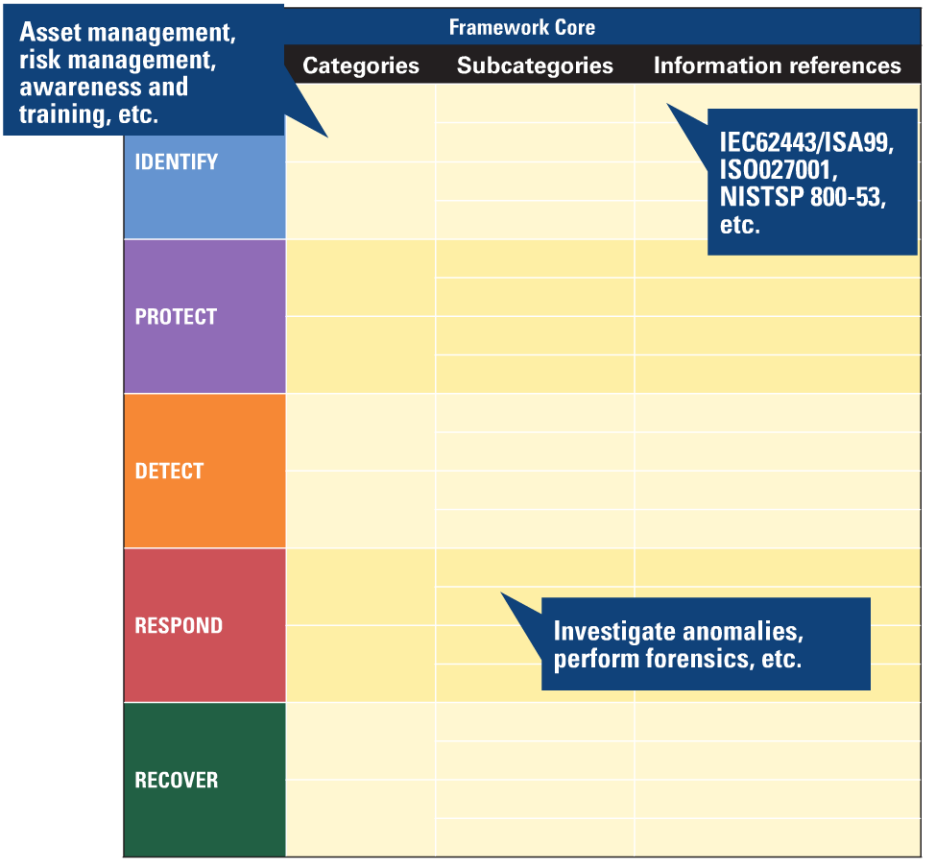
How the Framework Can Help Your Organization

The Cybersecurity Framework consists of three key parts:

- The Framework Core
- The Framework Profile
- The Framework Implementation Tiers

The Framework Core (Figure 2) helps provide an overview of the set of cybersecurity management activities that an organization is performing (or should be performing). Starting with five functions—identify, protect, detect, respond, and recover—the Core is divided into categories (such as asset management, risk management, awareness, and training) and subcategories (such as investigate anomalies and perform forensics). References (to sector, national, or international standard requirements or clauses) are then listed with these subcategories.

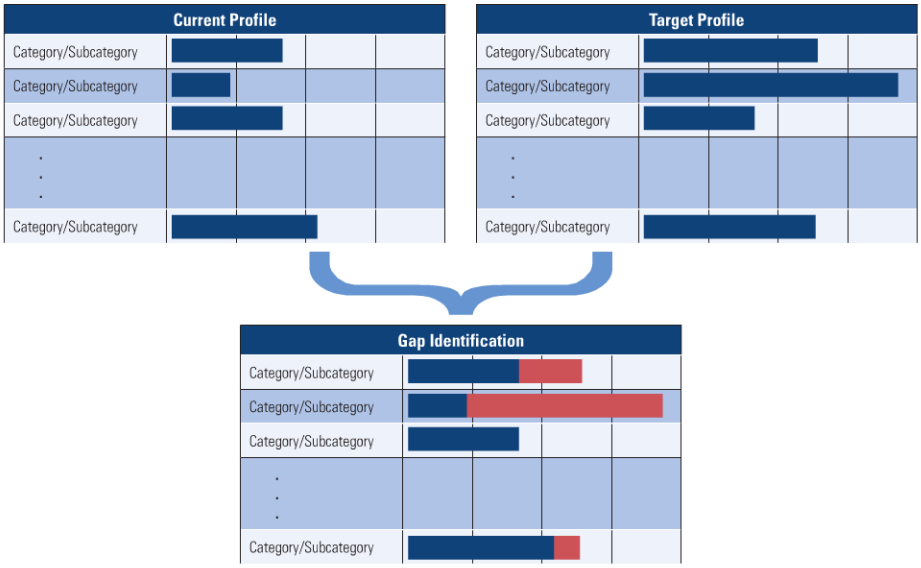
2. The Cybersecurity Framework Core. *Source: NIST*



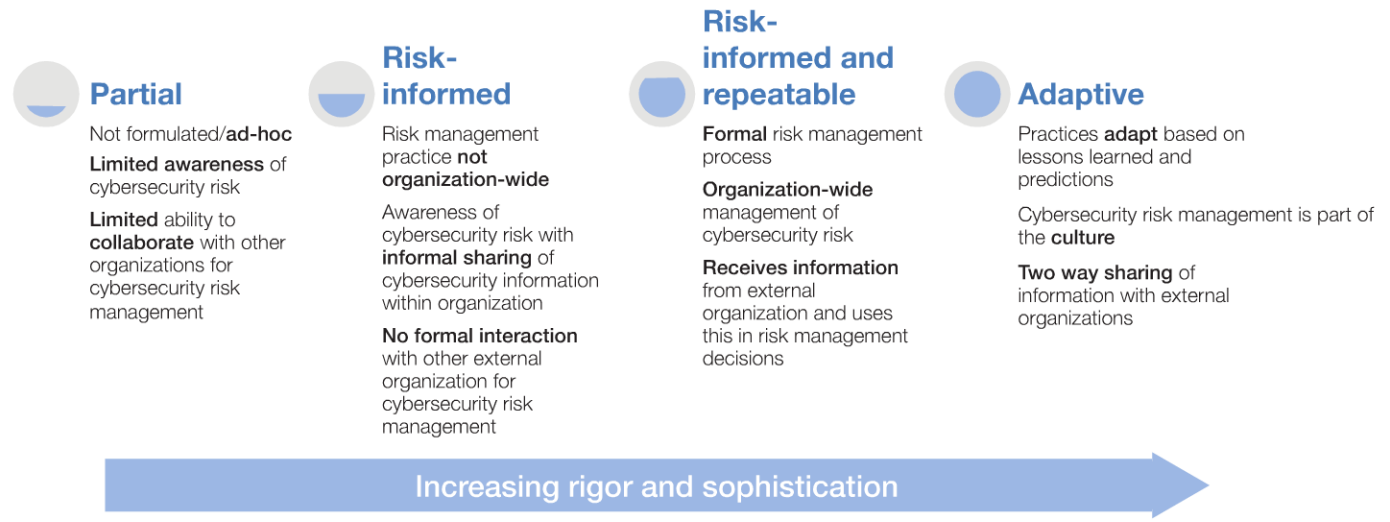
The Framework Profile (Figure 3) helps organizations quantify their desired outcomes when implementing the Framework Core. A "Target Profile" will show what the organization aims to achieve in terms of industry standards and common industry practices. The organization can then compare its "Current Profile" (what it is currently implementing and following) against the Target Profile to produce a gap analysis.

The Framework Implementation Tiers (Figure 4) help define how cybersecurity is managed within an organization. There are currently four tiers—partial, risk-informed, risk-informed and repeatable, and adaptive—which require increasing levels of rigor and

3. Gap analysis. Using the Framework Profile helps to identify gaps in an organization's cybersecurity implementation plan. *Source: NIST*



4. Move your organization forward. The Framework Implementation Tiers require increasing levels of rigor and sophistication. *Source: Steve Mustard*



sophistication to achieve. In general, the aim is for organizations to move from informal processes, which are not widely deployed in their business, to a culture of good cybersecurity practices supported by formalized and adaptable processes.

The Cybersecurity Framework will not automatically make an organization secure from cybersecurity threats. However, adopting the Cybersecurity Framework will help organizations be better prepared to deal with these threats, by providing:

- A high-level structure for an organization's cybersecurity management process.
- A focus on the appropriate application of standards.
- A view of an organization's cybersecurity management maturity.
- A common cybersecurity vocabulary.
- A clear statement to help senior management understand what their organizations need to be doing.
- Possible government incentives for adoption.

The intention of the Cybersecurity Framework in its current form is to help raise the overall level of cybersecurity preparedness across all sectors and businesses. This is especially important for those organizations that have so far done very little in this area. Even organizations that already have well-established cybersecurity management programs can benefit from adopting the Framework.

Electricity Sector Example

For a draft illustrative framework example for electricity sector industrial control systems, see http://1.usa.gov/1c3d3mx. The example acknowledges that this industry needs to accommodate a variety of legacy equipment that "requires special consideration when implementing cybersecurity practices."

The example also notes that, "Within the electricity subsector there are many stakeholders, including users, owners, and operators of the national power grid, as well as vendors, regulators and other interested parties. As such, there are many existing programs, guidelines, and standards, to leverage when creating a Framework Profile. Moreover, some organizations need to adhere to mandatory cyber security standards, such as the NERC CIPs. This Profile is written to be flexible and adaptable to different sizes and types of organizations within the electricity subsector, regardless of compliance obligations or existing programs."

What Should Organizations Be Doing?

Regardless of how well-established an organization's cybersecurity management program is, those with management responsibility should:

- Map out existing cybersecurity processes in the organization to produce a current profile.
- Review recommended industry, national, and international standards and identify a target profile that the organization should be following.
- Perform a gap analysis of the current profile against the target profile to identify actions to be undertaken to achieve the target profile.
- Review the actions and the target profile and either confirm or revise the target profile and required actions to achieve this revised profile.
- Raise awareness of cybersecurity management processes and procedures throughout the organization.
- Identify cybersecurity information-sharing channels within the sector and begin the process of establishing cybersecurity information-sharing processes.

In addition, organizations should consider engaging (if they have not already) in the Framework development process to help ensure that the Cybersecurity Framework remains relevant and valuable.

Next Steps

The Automation Federation has been actively involved in the development of the Cybersecurity Framework, helping to ensure that a focus is maintained on OT systems and ensuring that appropriate standards, such as ISA/IEC62443 (Industrial Automation and Control Systems Security), are applied.

On completion of the workshop phase of development, the Automation Federation and its member organizations are working with the White House and NIST on a series of tabletop exercises and seminars across the country to brief industry about the importance of adopting the Cybersecurity Framework. In addition, the Automation Federation's cybersecurity subject matter experts will continue to be engaged in the Cybersecurity Framework development process. ■

*—**Steve Mustard** (steve.mustard@au2mation.com) is an industrial control system and cybersecurity consultant. He is a Certified Automation Professional, member of the ISA, Fellow of the Institution of Engineering and Technology, and a member of the Automation Federation's Government Relations Committee.*