Promoting Interoperability Starts with Culture of Common Understanding

CIOs and CISOs should have a role in driving policy changes and technical changes.

James Mersol

Thu, 02/06/2020 - 09:27

Photo Credit: Gorodenkoff/iStock

As threats to information systems evolve, so do the frameworks, regulations and other defenses against those threats. While some solutions, such as the NIST cybersecurity frameworks and the Department of Homeland Security's CDM DEFEND task orders, are intended to give organizations the flexibility to choose the tools that both satisfy the requirements and integrate within existing systems, many organizations still struggle with choosing tools that work with one another.

According to a report published by CSIS’ Technology Policy Program, the average organization uses cybersecurity tools from 10 different vendors, many of which are not designed to work with one another. The result is a hodgepodge of programs that produce inefficient or redundant results or systems that require cybersecurity professionals or supplementary programs to manually translate data between tools.

In response, stakeholders seek to “develop an interoperable messaging format for cybersecurity tools” and “standardized data models and libraries to classify threats in a way that can be analyzed by any cybersecurity tool,” the report explains.

“The role of standards is a good place to start,” said Donna Dodson, chief cybersecurity advisor and fellow at the NIST Information Technology Laboratory, speaking on an interoperability panel at the Center for Strategic and International Studies (CSIS) Feb. 4. “When you think about something like the cybersecurity framework, you start to understand what outcomes you’re looking for and what standards help you get there.”

NIST looks for feedback from organizations that have had success with interoperability to figure out what lessons can be broadly applied within a framework, Dodson added.

“The problem grew out of the way the market developed,” explained Michael Daniel, president and CEO of the Cyber Threat Alliance and former cybersecurity coordinator in the Executive Office of the President.

Organizations typically buy security programs as “point solutions” to defend against one kind of malware; in response, few if any companies offer a comprehensive cybersecurity solution, and those that claim they do can only keep pace with threats for so long.

“Over the years, vendors got into this ‘my secret sauce is better than your secret sauce [model], and so I’m not going to cooperate with you,’” said Kent Landfield, chief standards and technology strategist for McAfee. “That cooperation is critical … for us to actually to be able to deal effectively with the problem.”

Both Landfield and Daniel said they would prefer a security landscape where vendors compete not over who has the best information on current and emerging threats, but on “higher-level” concerns, such as the cost of a solution or the quality of a company’s customer service.

“The consumers need to start driving the questions of the vendors,” he urged. “Do you interoperate, how, and why?”

Coincidentally, this discussion took place the day after the Iowa Caucuses, which were marred by delayed reporting and quality control errors centered around an app that had not been thoroughly tested.

“The situation in Iowa … is one of those classic examples of [how] technology does not always make things better,” Daniel said. “If you don’t actually combine it with processes and best practices in terms of how you conduct operations … it’s more an example of how not to bring technology in to a process.”

Training cybersecurity employees to rigorously test new technology, including through red teaming, is important to make sure everyone knows what to do when the solution breaks.

“You’re always going to have fits and starts when you roll out any kind of new technology,” Daniel said. “It’s almost predictable that this sort of thing would happen.”

Despite these visible hurdles in technology adoption and interoperability, the technical aspects are not the main obstacle going forward, the panelists said. As with many changes, effecting a culture shift is a necessary component, but also one of the most difficult ones. CIOs and CISOs must lead the change, requiring a shift in how they view their roles as well.

“We’re seeing some shifts within organizations in how they’re using technology,” Dodson said, “and that CIO/CISO community — how they can orchestrate for policy interoperability as well as technical interoperability instead of it just being ‘can I get the bits to get on the wire and communicate together?’”

Dodson warned that not bringing CIOs and CISOs to the table would exacerbate the problem as other offices purchase technology without thinking about how to integrate it into their existing architecture.

NIST is not a policy agency, Dodson emphasized, but it does think about how the policy community might react to its technical guidelines, trying to create an environment where policy enables technology modernization instead of hampering it.

The environment for adopting standards around interoperability must be “open and transparent,” Dodson said. “It has to be open so that you can have small and large players … come in and be able to understand the value add back to them.”

Transparency includes speaking to all stakeholders in terms that they understand, Dodson emphasized.

“We need to speak in plain English,” she said. “We need to be able to articulate this without having to read a 100-page treaty on what this means.”

The call to use plain English goes beyond publications, Dodson added, but is essential to communication with business to create better standards.

“When we are talking about capabilities, when we are talking about outcomes that we need to see in the cybersecurity … and privacy space … we [need to] have a common understanding of what these mean,” she emphasized. “From there, you can start to build common policies that from organization to organization you understand.”

Adopting a common understanding — or even ensuring everyone is on the same page with terminology and acronyms — not only enables communication about mission within organizations, but also gives smaller, innovative organizations the opportunity to introduce new solutions to longstanding problems like interoperability.

View printer friendly version
interoperability
Federal Cybersecurity
NIST
Standard