FORTRA™

WHITE PAPER (TRIPWIRE)

Closing the Integrity Gap with NIST's Cybersecurity Framework

Implementing a Practical Roadmap to Identify and Manage Cyber Risk Against Escalating Threats—And Bring Integrity Management Into Sharper Focus

When the National Institute of Standards and Technology (NIST) announced that it had released its new Cybersecurity Framework in 2014, it appeared on the surface to be just one more option for organizations looking to develop a cohesive and effective cyber risk management strategy. Indeed, there are dozens of choices available and organizations have been all over the map when it comes to deciding which compliance frameworks and which tools they should use to support the variety of security standards available.

NIST's Cybersecurity Framework is unique, however. For starters, it was developed by NIST in partnership with organizations from the critical infrastructure industry to address complex cybersecurity challenges within operational technology environments, such as manufacturing, utilities, energy, transportation, health care and chemicals. The Framework was designed to simplify an organization's approach to securing these and other complex environments, yet it is universal in scope. Importantly, it provides a common language that helps all personnel—from the IT team to department heads and other decision-makers within the C-Suite—define and understand security problems and potential solutions within the context of the overall mission. It then offers flexible guidance to help organizations from every industry meet their specific business objectives from the top down.

It is not a one-size-fits-all approach. Organizations face different threats and have different vulnerabilities and different risk tolerances. With the NIST Cybersecurity Framework, they can pick, customize and prioritize which practices and activities will help them reduce and better manage their unique cybersecurity risks and gain the fastest time to value.

These characteristics are part of why an increasing number of private sector companies are diving deeper into NIST Cybersecurity Framework adoption. Gartner predicted that 50% of all U.S. organizations would be using this framework by 2020.[1] Meanwhile, the framework has been adopted by various countries as part of their cybersecurity strategy; and in some cases, their national legislation.

"The full maximum NIST Cybersecurity Framework is about as big an umbrella as you are going to find," says Edward G. Amoroso, CEO for TAG Cyber.

Amoroso recommends to companies, "… if you're going to pick something, you might as well pick the thing that has everything"—a suggestion he also made to the Trump Administration prior to the release of the May 2017 Presidential Executive Order (EO) on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which mandates all government agencies to use the NIST Framework for managing risk.

Because the NIST Framework facilitates a risk-based approach, it also heightens the awareness of cyber threats across the organization, accelerates the efforts to create a stronger cybersecurity strategy and supporting program, and it can reduce the possibility of miscommunications between staff of other functions that integrate with cyber departments.

First developed by the executive order of President Obama in 2013, the Framework became a requirement for all federal agencies by order of President Trump in May 2017. A new version was issued in late 2017.

"NIST is probably the most thoughtful, comprehensive, well-researched, accepted framework out there," says cybersecurity technology officer David Meltzer. "It's robust enough to complement what large organizations are already doing in cyber, but flexible enough to give smaller organizations a roadmap to improved cybersecurity.“

New Threats, Different Vulnerabilities

More urgently, perhaps, is the immediate need for critical infrastructure and other companies to successfully prepare for the anticipated increase in integrity-related threats.

Global ransomware is an integrity-related threat, for example, and its costs, alone, will reach $20B in 2021, which is 57x more than it was in 2015, according to leading research firm, Cybersecurity Ventures.[2]

"Integrity is really at the heart of information security protections for any system," says Ron Ross, Fellow for NIST. "Because if someone is able to indiscriminately change an application or a piece of data or the BIOS instructions or anything within the computing stack—whether the customer is aware or not aware of those changes—then that really attacks the basic underpinnings of an information system, along with everyone's trust in it."

The consequences of an integrity-related attack are devastating for any organization, but especially those that handle critical infrastructure systems. If an attacker manages to tamper with a medical device, the critical safety system of an automobile, the data collected during a clinical trial or the operations of a power plant—the result could be major disruption or even death.

Says Amoroso, "Unfortunately, most security experts, including myself, are predicting that the shift towards integrity-oriented threats is coming like a tsunami and most organizations are poorly set up to stop those types of things."

Organizations of every size—and in every industry—can improve their ability to protect critical assets and operations against these types of attacks by utilizing the NIST Cybersecurity Framework, which is designed to be easily paired with an organization's choice of security control catalogs like NIST 800-53, ISO 27000 and the Center for Internet Security Critical Controls to enable strong integrity management, including configuration management, file integrity monitoring and change management.

And that's because it's no longer simply a question of vulnerability and defending data and systems against any penetration by an outside-in intrusion, states Ross. "You are going to be hit at some point, if you haven't been hit already," he says. "So the important thing is not to keep worrying about the likelihood of an adversary attack. It's: Do they have the capability of attacking you, and what would be the impact if that happens?"

The *How* of Identifying Risk

The best time for that discussion is before an attack occurs, and NIST's Cybersecurity Framework is designed to force organizations to triage their critical systems based on the negative impact an attack would have on their mission or business.

"There are things that are low impact, moderate impact and high impact, and once you figure out what's most critical, then you can actually engineer and apply all of the security tools and security controls and best practices in a way that's really focused on those most critical assets," says Ross. "Then everything else you can kind of let go and be less rigorous in that process."

To do this, the Cybersecurity Framework features a set of core activities, outcomes and applicable references that are easily understood and communicated from front line operations to the executive level. These are all contained within five overarching functions, each of which can be further broken down into categories and subcategories.

- **Identify**—This function allows organizations to better understand the business context and the resources that support critical functions, and the related cybersecurity risks so it can focus and prioritize its efforts, consistent with its risk management strategy and business needs.
- **Protect**—By helping organizations to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services, this function supports the ability to limit or contain the impact of a potential cybersecurity event.
- **Detect**—With this function, organizations develop and implement the appropriate activities to enable the timely discovery of a cybersecurity event.
- **Respond**—This function supports the ability to contain the impact of a potential cybersecurity attack by developing and implementing response activities.
- **Recover**—This function supports the timely recovery to normal operations to reduce the impact from a cybersecurity event.

According to NIST, these five functions aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats and improving by learning from previous activities. They also align with existing methodologies for incident management and help show the impact of investments in cybersecurity.

That the functions are described using basic, plain English terminology is no coincidence. "All of these words are meaningful for cybersecurity risk management but they're also meaningful for larger risk discussions," says Matthew P. Barrett, Program Manager for the NIST Cybersecurity Framework. "This really stages cybersecurity for consideration in those larger enterprise risk discussions. It sounds simple, and in some respect it really is, but it's an incredibly important extra step that's available in our framework and not in others."

Although the steps can be utilized concurrently and continuously, NIST recommends that organizations spend a lot of upfront time on the "Identify" task.

"That's the step that helps you gain context," Ross says. "How are you going to organize your organization to build the best security program you possibly can? What is your risk management strategy? What are your critical assets? What are the different things you do in your mission and business space that need to be addressed? What kind of IT assets do you have now? All of that has to be organized first, to understand where you're going in the future with regard to what kind of program you're going to build with regard to security."

These five functions also allow organizations to take a "dip your toe in the water" approach. "You don't have to do a 50-page business plan out of the gate. We don't have to have an expensive risk authority matrix or policy library in order to do governance or a tome on cybersecurity risk management strategy," explains Barrett. "You can do all of those thing with a page or less of paper and just capture it for the future and communicate it within the business, so everyone knows what solid ground looks like. Then you can move deeper into categories and subcategories within each function."

How Tripwire Maps to the NIST Cybersecurity Framework

Why do companies consider Tripwire functionality a key component to successfully implementing the NIST Cybersecurity Framework? Because the controls found in Tripwire solutions provide support for all five functions of the Framework, including integrity controls specific to 13 of the Framework's subcategories.

FUNCTION	CATEGORY
Identify	Asset Management • Physical devices and systems are inventoried • Software platforms and applications are inventoried
	Risk Assessment • Asset vulnerabilities are identified and documented • Threat and vulnerability information is received from information sharing forums and sources • Potential business impacts and likelihoods are identified • Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
Protect	Access Control • Network integrity is protected, incorporating network segregation where appropriate
	Data Security • Integrity checking mechanisms are used to verify software, firmware and information integrity
	Information Protection Processes and Procedures • A baseline configuration of information technology/industrial control systems is created and maintained • Configuration change control processes are in place • A vulnerability management plan is developed and implemented
Detect	Security Continuous Monitoring • Vulnerability scans are performed
Respond	Analysis • Forensics are performed
Recover	Restore systems in a timely fashion using remediation guidelines/advice derived from Tripwire policy content

Going Vertical

Once organizations set a foundation with the NIST Cybersecurity Framework, they can easily pivot to using NIST Special Publications like 800-53, 800-160 and 800-171 or another comprehensive security control catalog and further bolster their ability to manage their systems for integrity-related changes and attacks.

Historically, the security focus has been on protecting data confidentiality and system availability, or the "C" and "A" components of the "CIA Triad." Of lesser priority has been integrity—the "I" in the strategy—which is focused on protecting data and systems from modification or deletion by unauthorized parties and ensuring that damage can be repaired or reversed. In today's environment, though, cyber attackers are much more likely to exploit a system's integrity—or lack thereof. In doing so, they can not only change and modify coding and operational settings, but they can also steal intellectual property and customer information and shut down systems. All of this illustrates that there is an inherent relationship between a system's integrity and its confidentiality and availability.

"Integrity is critical because once you establish a certain lockdown set of configuration settings or you deploy software, adversaries like to get into your systems and networks and they like to attack your systems and deploy unauthorized, malicious code," says Ross. "Thus, you have got to understand what's on the network and make sure that any changes to that network are done by authorized individuals so that you have really strict control over the configuration settings and also any changes to software and systems that go on routinely within organizations."

Integrity management involves a number of capabilities including those safeguards or countermeasures designed to continuously assess hardware and software vulnerabilities, passively and actively monitor in real-time to identify and report on weaknesses and support incident investigation and mitigation. By pairing NIST Cybersecurity Framework guidance with specific NIST controls, organizations across all industries and risk profiles can ensure that they are effectively addressing these capabilities. When implemented properly, integrity management can prevent the majority of breaches from happening.

NIST SP 800-53, a catalog of security and privacy controls, includes a number of control families that deal specifically with integrity. Together, the 800-53 controls include guidance and tools for capabilities that help manage and ensure system integrity including log management, configuration management, vulnerability management, change management and asset management.

Of course, security controls have long been available to and used by information security teams, but when used within the context and roadmap of the NIST Cybersecurity Framework, they can be linked and mapped up through the Framework's pyramid shape of detailed safeguards, subcategories, categories and functions and then conveyed to the C-Suite.

"It's a beautiful way to get that communications started, going both up and down the organizational hierarchy, to make sure that integrity is an issue that is recognized as important and well-defined at the boardroom level," says Ross. "This is really critical: Integrity has to be a primary objective of the C-Suite, to the people at that level, if integrity is going to be a part of the overall security discussion and prioritized in the security strategy and the successful implementation of that strategy."

Easing Integrity with Tripwire

Extending integrity management to the full range of critical infrastructure assets managed will enable you to reduce your organization's overall attack surface and address more cumulative security and operational risks. To that end, Fortra's Tripwire offers an integrated suite of foundational controls that deliver integrity assurance closely aligned with NIST guidance, including the Cybersecurity Framework and SP 800-53, Revision 5. In fact, Tripwire has released an expanded platform and policy support for NIST 800-53 and has addressed a number of its specific requirements, including:

- Automation of the implementation and management of security controls
- A continuous monitoring capability
- Ease of reporting in support of annual reviews
- Specific support of configuration management family of controls, system integrity requirements and information system monitoring

Specifically, Tripwire’s Industrial Security Solutions suite provides a holistic set of software applications that assess, harden and monitor plant and industrial environments to drive availability, safety and resilience against cyber incidents that could adversely impact operations.

“In so many ways, Tripwire is better positioned than most cybersecurity vendors to provide the critical components of good, solid foundational cybersecurity programs… from asset identification to vulnerability assessment to change identification and impact,” says Meltzer. “They’ve got the tools that work together to solve integrity management challenges and they can do it at a scale better than most. So, they are uniquely positioned in a lot of ways to respond to the breadth of the NIST expectations for critical infrastructure organizations and beyond.”

Sources

1 https://www.oas.org/en/sms/cicte/docs/OAS-AWS-NIST-Cybersecurity-Framework(CSF)-ENG.pdf

2 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We’re creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We’re the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.