ACHIEVING SECURITY

with the

NIST CYBERSECURITY FRAMEWORK

INDUSTRY PERSPECTIVE

DELL

INTRODUCTION

Cyberthreats present serious, ever increasing risks to federal agencies. An April 2014 Government Accountability Office report notes that federal agencies reported 64,214 information security incidents to the U.S. Computer Emergency Response Team (US-CERT) in 2013, a 104 percent increase from 2009. Government has responded through legislation, executive orders, and cross-agency priority (CAP) goals that put cyber at the top of its agenda. However, with thousands of employees, siloed departments, and tight budgets, improving agency cybersecurity while maintaining mission-critical operations is a major challenge.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework – an outline developed by government and industry leaders to identify, analyze, and consolidate standards and practices for cyber risk – can help organizations meet these needs.

In GovLoop's latest industry perspective, we explore the following:

- Origins and development of the Framework
- The three components, Core, Profile, and Implementation Tiers, that comprise the Framework
- How it benefits agencies and addresses common challenges to cybersecurity
- Tips for agency implementation
- How Dell – a major supporter of the Framework and a contributor to ongoing public discussions surrounding it – can help federal agencies and other organizations adopt the Framework to improve their cybersecurity posture, with an emphasis on identity and access management and network security

To gain valuable insight into these topics, we spoke with:

- Matthew Barrett, Program Manager, NIST
- Paul Christman, Vice President, Federal, Dell Software
- Danielle Kriz, Director, Global Cybersecurity Policy, Information Technology Industry Council (ITI)

GOVERNMENT CYBERSECURITY CHALLENGES

According to a Government Business Council (GBC) report, funding constraints, slow technology acquisition processes, bureaucratic inertia, and the need to comply with multiple federal mandates are significant challenges that agencies face in securing their networks.

Agency siloes are also problematic. Many security measures were established before cloud technologies were adopted, so former IT departments locked down individual parts of the network to secure them. This siloed approach created gaps in network architecture, forcing IT administrators to manage each silo separately. This approach increased costs and risk, as well as difficulty for the user.

To more effectively address cybersecurity, a simple yet comprehensive approach is needed. The NIST Cybersecurity Framework provides a holistic view of an organization's network that improves security while sustaining business functions.

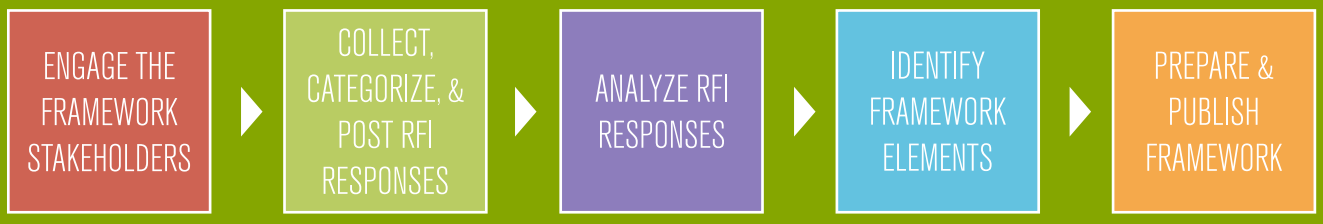
ORIGINS OF THE FRAMEWORK

In accordance with Executive Order 13636, Improving Critical Infrastructure Cybersecurity, NIST released the Framework in February 2014. The strategy provides a way to tackle cyberthreats while protecting citizens' privacy and civil liberties. It is not meant to replace any existing policies or regulations. Instead, it lays out a way to assess and address an organization's susceptibility to cyberattacks. Compliance with the Framework is voluntary, but would be beneficial to any organization.

Based on the executive order, the Framework must:

- "Include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks;
- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk;
- Identify areas for improvement to be addressed through future collaboration with particular sectors and standards-developing organizations; and
- Be consistent with voluntary international standards.

DEVELOPMENT OF THE FRAMEWORK



- **Feb. 12, 2013:** EO 13636 issued
- **Feb. 26, 2013:** NIST Issues RFI
- **Apr. 30, 2013** 1st Framework Workshop
- **Apr. 08, 2013:** RFI Responses Due
- **May 15, 2013:** Identify Common Practices/Themes
- **May 2013:** 2nd Framework Workshop at CMU
- **June, 2013:** Draft Outline of Preliminary Framework
- **July 2013:** 3rd Workshop at UCSD
- **Sept. 2013:** 4th Workshop at UT Dallas
- **November 2013:** 5th Workshop at NC State
- **Feb. 2014:** Published Framework

*ONGOING ENGAGEMENT: Open public comment and review encouraged and promoted throughout the process.

DEVELOPING THE FRAMEWORK

NIST recognizes that there is no one-size-fits-all model for managing risk. The agency created the Framework to be adaptable to any sector, technology infrastructure, or risk environment. The development of the Framework was – and continues to be – a collaborative, iterative effort between government, industry, and academia.

"This process was even more interactive than our normal NIST process," said Matthew Barrett, Program Manager at NIST, in an interview with GovLoop. "We had five workshops in five different cities in less than a year to try to get the broadest perspective possible of what the Framework should and shouldn't be."

IDENTITY & ACCESS MANAGEMENT

The FY 2014 Federal Information Security Management Act (FISMA) compliance report paints a gloomy picture of federal IT security. Several agencies have made no progress in meeting the Strong Authentication CAP goal, and fifteen agencies have yet to reach even 50 percent implementation. This is problematic, especially since US-CERT reported that 52 percent of cybersecurity incidents in FY2014 were related to or could have been prevented by Strong Authentication CAP implementation.

NIST supports the development of better identity and authentication solutions through its participation in the National Strategy for Trusted Identities in Cyberspace (NSTIC), as well as its partnership with the Identity Ecosystem Steering Group (IDESG).

Within the Framework, there are several Functions and Categories that relate to identity and access management (IAM). For example, within the Protect function, there is the category of Access Control. This category breaks down into five subcategories:

- PR.AC-1: Identities and credentials are managed for authorized devices and users
- PR.AC-2: Physical access to assets is managed and protected
- PR.AC-3: Remote access is managed
- PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties
- PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate

"There's the intersection between identity and access management and network security," said Dell's Paul Christman. "The major driver that is requiring network security and identity and access management to come forward now is mobility. Mobility is creating this idea that work isn't a location – work is a function."

For example, think of a Health and Human Services caseworker doing field inspections. In the past, the caseworker would go to a field location, fill out an inspections form, go back to his office, and input the information on a desktop. Today, however, technology is becoming as mobile as the work and the user, and subsequently, these devices need to be incorporated into security.

"The idea of 'remote' is always present in the Framework," said Christman. "Just focusing on perimeter protection is really a non-starter these days. It's important to recognize that access control and network security are in the same category."

Similarly, it is important to see identity and access management not just as an IT issue, but a business one.

"We're trying to emphasize the idea that the line of business should define what applications an employee has access to," said Christman. "This is a fundamental shift away from identify and access management being an IT function, to it being a business function."

THE FRAMEWORK AT A GLANCE

The Framework consists of three components: Core, Profile, and Implementation Tiers. Each component reinforces the connection between business drivers and cybersecurity activities.

CORE

The Core is a lexicon of information security program management mechanisms that are common across critical infrastructure sectors. At the highest level, it identifies five security Functions – Identify, Protect, Detect, Respond, and Recover. The Core gets more detailed as it works its way down through Categories, Subcategories, and finally, Informative References. For example, within the function Identify, there is the category Governance, which has a subcategory Organizational information security policy is established, which then provides four Informative References as examples of what an organization should consider implementing.

"[The Framework Core] gives us a language which we can use to talk with each other about cybersecurity," explained Barrett. "There are all sorts of ways risks manifest, and one of those ways is miscommunication. The Framework Core is a great mechanism to make sure that we're using a universal language when we're talking about information security program management."

Organizations can use the Framework Core to reflect on important questions such as ask the following questions:

- What assets need protection?
- What safeguards are available?
- What techniques can identify incidents and contain their impacts?
- What techniques can restore capabilities?

PROFILE

According to NIST, the Profile is a customization of the Core for your organization. It enables organizations to establish a roadmap for reducing cybersecurity risk. It also considers legal and regulatory requirements, industry best practices, and risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles aligned with particular components and needs.

"A Profile is a way of taking the Framework Core and putting it on a scale. You can measure where you're at now and quantify where you might like to be a year or five years from now," Barrett said. "In other words, the Profile is applying the Framework Core for gap analysis. The Profile then helps you decide which of those gaps need to be addressed first, according to mission priorities."

IMPLEMENTATION TIERS

Implementation Tiers consider an organization's current risk management practices, threat environment, legal and regulatory requirements, objectives, and constraints. The Tier characteristics are measured at an organizational level to understand the current state of a given risk practice. Feedback from stakeholders during the Framework's development indicated the need for flexibility in implementation and concepts of maturity models. Therefore, the Tiers are progressive, beginning with (1) Partial, then (2) Risk Informed, (3) Repeatable, and (4) Adaptive.

"While they do build on each other, the Tiers weren't necessarily designed such that everybody needs to strive for a 4 on the 1 to 4 scale," Barrett explained. "The Tiers themselves are meant to facilitate a tradeoff analysis dialogue about what is most appropriate for a given organization because we recognize – as industry was informing us – that there's a cost to doing business and to various decisions regarding how you manage risk."

BENEFITS OF THE FRAMEWORK

There are many benefits to the NIST Cybersecurity Framework. Through being neutral, broadly applicable, vetted by industry, and engaging to stakeholders, the Framework can reduce time and expense of starting an information security program and also reduce risk within current programs by identifying areas for improvement.

NEUTRAL & BROADLY APPLICABLE

"The thing that we like about the NIST Framework is that it is neutral," said Christman. "It's neutral to mission of organization, to industry, and to data type."

Although it can be used with specific data types or objectives in mind, the Framework is a much broader approach to security. Therefore, its benefits can be realized by a variety of organizations, such as hospitals, civilian federal agencies, educational institutions, defense agencies, commercial enterprises, and more.

"The other thing that we like about the Framework is that it's neutral to threat factor," Christman continued. "It could be a trusted insider threat, an advanced persistent threat from a nation state, or a malicious hacker. The threat factor is really not the issue. Regardless of mission, industry, data type, or threat factor, your organization can improve its security posture."

VETTED BY INDUSTRY

The Framework is also beneficial because it meets industry-vetted criteria. According to the Information Technology Industry Council (ITI), a high-tech trade association based in Washington, D.C., an effective cybersecurity effort should:

- Leverage public-private partnerships and build upon existing initiatives and resource commitments
- Reflect the borderless, interconnected, and global nature of today's cyber environment
- Be able to adapt rapidly to emerging threats, technologies, and business models
- Be based on effective risk management
- Focus on raising public awareness
- Focus on bad actors and their threats

"The Framework is the right approach because it hits almost all of those guiding truisms," said Danielle Kriz, Director of Global Cybersecurity Policy at ITI. "It's globally workable and it leverages already existing standards and best practices that were developed by industry."

ENGAGING TO STAKEHOLDERS

The NIST Framework helps organizations communicate their cybersecurity requirements with stakeholders, including partners and suppliers. It is a good way to start a discussion with technical and non-technical stakeholders to further the security posture of organizations.

"The beauty of the Framework is we can drill down into the finite details. But at a very high level, I could explain what it means to a business person in a line of an agency or an educational institution, and help them understand what needs to happen because it can be explained in plain English," Christman said. "We can use this Framework to connect the stakeholders – the people with access to money, people, and resources – and connect the technical, policy, and governance issues."

IMPLEMENTING THE FRAMEWORK

As required by Executive Order 13636, the Framework is flexible, so that the adopting agency can utilize it as it sees fit. For example, it is nearly impossible to administer an absolute "yes or no" regarding the Subcategory, "Physical access to assets is managed and protected," within the 'Protect function' and 'Access Control' category. Therefore, each organization must judge satisfactory fulfillment of a given Category or Subcategory. Each organization must also decide how to measure the extent of that fulfillment.

"Herein lies the flexibility of how you apply the Framework. You can set up your own scale by which you're going to measure yourself," said Barrett. "There's a lot of flexibility there and it's purposely left that way."

Given this flexibility, however, organizations must make honest self-assessments of their current level of security.

"The NIST Framework doesn't tell you what to buy. It won't tell you, 'This is the product, vendor, or consultant you need to hire,'" said Paul Christman of Dell. "It really is an opportunity for healthy inspection and reflection, and also a prudent plan with a lot of very thoughtful technical details under the covers."

As a result of this comprehensive review, an organization's security blind spots are often revealed. "Think of [the Framework] as a checkup to make sure that you're covering all things – not only the things that you've accomplished, but also think of it as a continuous improvement tool that you can reference," Christman said.

Based on NIST and Dell recommendations, there are seven steps to using the Framework:

1. Prioritize and scope mission objectives and priorities per the Identify, Business Environment category (ID.BE).
2. Match critical systems with threats.
3. Align and resolve conflicting security requirements using the Framework Core as your organizing construct.
4. Apply your mission priorities (expressed in the course of reflecting on the Business Environment category, step 1) to your security requirements in step 3, creating a Framework Profile for your organization to use as a benchmarking tool.
5. Create a target Profile of the organization's desired state.
6. Determine, analyze, and prioritize gaps between mission priorities, critical systems, current technology profile, desired state, and risks.
7. Develop a strategy to address the items uncovered in step 6.

HOW DELL CAN ENSURE AN EFFECTIVE CYBERSECURITY IMPLEMENTATION

The Framework holds great promise, but the tools and processes implemented will determine agencies' cybersecurity readiness and mission success.

While an organization may have compliant infrastructure and processes already in place, it is likely that additional steps will be needed to further satisfy Framework requirements and improve security posture. Dell offers solutions that a Framework-compliant organization requires such as servers, storage, desktops, laptops, and mobile devices. They also provide services and software to help an organization optimize, migrate, and manage its IT infrastructure. Device encryption and patching, network security, next generation firewalls, and identity and access management are just a few of the components comprising a holistic, connected security implementation.

"Dell looks at security as a series of interconnected technologies," said Christman. "And we are the only organization that has both the hardware and the software stack to make this connected security actually happen. We think it's a major competitive advantage for us to stitch together all these different parts. Nobody in the industry can cover as much of the NIST Framework as we can."

CONCLUSION

The NIST Cybersecurity Framework is an outline, not a prescription. It does not tell an organization how much cyber risk is tolerable, nor does it claim to provide the one and only formula for cybersecurity. Instead, it provides a common language and systematic methodology for managing cyber risk. By having a common lexicon to enable action across a very diverse set of stakeholders, the Framework will allow the best practices of elite companies to become standard practices for everyone.

The Framework is also a living document. It will be updated over time as stakeholders learn from implementation and as technology and risks change. The Framework focuses on questions an organization needs to ask itself to manage its risk, because, while practices, technology, and standards will change over time, principles will not.

"NIST plans to continue outreach with an eye toward self-sustaining communities and making the relationship between cyber risk management and larger risk management practice better understood and more seamless," Barrett said.

After all, cybersecurity is a shared responsibility. The responsibility doesn't just lie with the tech sector, or industry, or government. It lies with everyone.

To uphold this critical responsibility, the Framework can guide the way.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 150,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C. with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to: Catherine Andrews, GovLoop Director of Content, at Catherine@govloop.com.

1101 15th St, NW, Suite 900
Washington, DC 20005
Phone: (202) 407-7421
Fax: (202) 407-7501
www.govloop.com
@GovLoop

ABOUT DELL

Dell empowers countries, communities, customers and people everywhere to use technology to realize their dreams. Customers trust us to deliver technology solutions that help them do and achieve more, whether they're at home, work, school or anywhere in their world.
www.dell.com

FUNCTION & CATEGORY UNIQURE IDENTIFIERS

FUNCTION	CATEGORY	DELL SOLUTIONS
IDENTIFY	ASSET MANAGEMENT BUSINESS ENVIRONMENT GOVERNANCE RISK ASSESSMENT RISK MANAGEMENT	• SUPPLY CHAIN ASSURANCE • DELL ONE IDENTITY (IDENTITY & ACCESS MANAGEMENT • – IAM) • INSIDER THREAT SERVICES
PROTECT	ACCESS CONTROL AWARENESS TRAINING DATA SECURITY INFO PROTECTION PROTECTIVE TECHNOLOGY	• DELL ONE IDENTITY • KACE SYSTEMS MANAGEMENT • DELL DATA PROTECTION|ENCRYPTION (DDP|E) • CLOUD CLIENT COMPUTING • ARCHIVE SOLUTIONS • INFORMATION ASSURANCE (IA) CYBERSECURITY LAB • SUPPLY CHAIN ASSURANCE • SECUREVIEW WORKSTATIONS • SONICWALL NETWORK SECURITY & SECURE MOBILE • ACCESS • MONITORING • APPASSURE BACKUP AND RECOVERY • NETVAULT BACKUP AND RECOVERY • BACKUP HARDWARE • INSIDER THREAT SERVICES
DETECT	ANOMALIES & EVENTS CONTINUOUS MONITORING DETECTION PROCESSES	• DELL ONE IDENTITY • SONICWALL NETWORK SECURITY & SECURE MOBILE • ACCESS • CLOUD CLIENT COMPUTING • INSIDER THREAT SERVICES • KACE SYSTEM MANAGEMENT
RESPOND	COMMUNICATIONS ANALYSIS MITIGATION IMPROVEMENTS	• INSIDER THREAT SERVICES • OTHER SECURITY SERVICES (INCLUDING SECUREWORKS)
RECOVER	RECOVERY PLANNING IMPROVEMENTS COMMUNICATIONS	• APPASSURE BACKUP AND RECOVERY • NETVAULT BACKUP AND RECOVERY • BACKUP HARDWARE

1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
@GovLoop