Protecting Your Most High-Value Assets with the NIST Cybersecurity Framework

RESEARCH BRIEF

"Cybersecurity threats continue to exploit the increased complexity and connectivity of critical infrastructure systems, placing the nation's security, economy and public safety and health at risk."

NIST CYBERSECURITY FRAMEWORK

Executive Summary

The Trump administration is doubling down on protecting our nation's most critical assets by enhancing the government's cyber posture. In May 2017, the President issued an executive order titled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Additionally, the fiscal 2019 budget highlights integrating cybersecurity into every aspect of IT modernization and making it a priority at all federal agencies.

To meet these mandates and obligations, agencies are turning to the National Institute of Standards and Technology's Cybersecurity Framework. NIST developed the CSF in collaboration with industry and government to set standards, guidelines and best practices to promote the protection of critical infrastructure and improve government security. It is now a mandate that agencies must meet under the current administration.

The CSF Core is a "set of cybersecurity activities, desired outcomes and applicable references common across critical infrastructure sectors." The core consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond and Recover.

We've previously talked about adopting the CSF and identifying your most valuable assets and data. Now it's time to discuss the next phase, Protect, which ensures that data at rest and in transit is secure.

To learn more about the CSF's usage, perception and outcomes in government, particularly its Protect function, GovLoop teamed with cybersecurity firms Symantec and DLT to survey 79 federal employees. Only 40 percent of respondents said they have implemented the CSF, and another 27 percent are just getting started since the release of the President's cybersecurity executive order. (See Figure 1).

To gain additional insights, GovLoop sat down with Ken Durbin, CISSP Senior Strategist of Global Government Affairs and Cybersecurity at Symantec, and Don Maclean, Chief Cybersecurity Technologist at DLT.

There are many reasons why agencies have yet to properly implement the CSF guidelines. In this research brief, we discuss them in addition to common challenges to protecting your agency's most critical assets, how you can improve data loss prevention and how to procure new solutions that align to your cyber strategy and the CSF.

FIGURE 1

Per the President's executive order on cybersecurity released in May 2017, has your agency implemented the NIST Cybersecurity Framework (CSF)?

- **Yes, we are well underway 40%**
- **Yes, we just started 27%**
- **No, but we plan to 9%**
- **No, we don't have a timeline for implementation 24%**

5 key functions of the CSF

The Impetus to Protect

The most recent Federal Information Modernization Security Act report, issued to Congress in 2016, shows 30,899 reported cyber incidents that led to the compromise of information or system functionality that year. What's more, attacks using ransomware are getting costlier for the government. While the average ransomware demand actually decreased in 2017 to $522, the number of ransomware variants increased by 46 percent. Additionally, 5.4 billion WannaCry attacks were blocked.

For 2018 and beyond, the pressure is on federal agencies to make sure they are doing their utmost to protect critical assets. Within 30 days of the Final IT Modernization Report, NIST was tasked with providing the Office of Management and Budget with "a plan to promote a risk management culture that focuses agency effort on the operational performance and compliance of their most valuable systems."

The goal of the CSF's Protect function is to "develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event." Methods include identity management and access control, awareness and training, data security, maintenance and protective technology.

For example, implementing two-factor authentication for employee devices is a simple and significant first step to meeting the protection requirements. Fortunately, agencies are already prioritizing it. According to our survey, about 93 percent of federal respondents have at least explored the Protect function (See Figure 2).

Additionally, about 76 percent of respondents said they believe their agencies ensure that systems are configured to provide only necessary services to end users in a "least functionality" manner. (See Figure 3).

But to meet the Trump administration's recent mandates and stay ahead of malicious attackers, it's critical to take "exploring the Protect function" to the next level. "Cybersecurity threats continue to exploit the increased complexity and connectivity of critical infrastructure systems, placing the nation's security, economy and public safety and health at risk," the CSF states.

Agencies must step up their efforts not only in implementing the overall CSF, but also in following through with the Protect function. Federal officials seem to understand the importance of prioritizing the protection of critical assets and data. Our survey shows that about 81 percent of respondents believe they correctly prioritize their agency's protection efforts. (See Figure 4).

Regardless of where your agency stands in prioritizing the CSF's Protect function, the impetus is clear: Cybersecurity attacks are increasing in number and complexity, and agencies stand to lose too much money and public trust to fail at defending the nation's critical infrastructure.

FIGURE 2

Has your agency explored the "Protect" function of the NIST Framework? The "Protect" function can be used to ensure your agency's high value assets are properly secured.

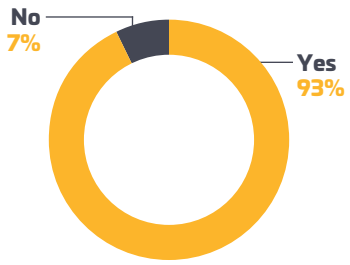


FIGURE 3

Does your agency ensure that systems are configured to provide only necessary services to end users? ("least functionality")

FIGURE 4

Do you believe your agency correctly prioritizes protection efforts?

The Need for Data Loss Prevention

Keeping sensitive information safe and compliant is never easy. But it becomes even more challenging when sensitive information leaves the safety of your agency's networks, as more employees share files via cloud storage services and access those files on various mobile devices. How do you manage and protect your agency's information in this challenging environment?

A critical component to protecting your agency's high-value assets is first preventing data loss. Data loss prevention, or DLP, is defined as technologies that counteract the loss of data. DLP technologies can protect data at rest, on premises or in cloud applications; in motion over the network; or on a managed endpoint.

DLP also helps protect personal data by ensuring who has access to it, where it is located and how it is used. Specifically, DLP technologies can do this by automatically encrypting sensitive data before it's sent, even when the sender forgets to encrypt the data.

Government understands the importance of investing in data protection and preventing data loss. According to our survey, 70 percent of federal respondents use DLP to control what data end users can transfer or share outside their agency's networks. (See Figure 5). Of those, about 67 percent say that their DLP tools protect sensitive and high-value data both on premises and in the cloud. (See Figure 6).

Executing DLP can range from simple notifications to active blocking, all based on policy and rules defined to address the risk of inadvertent or accidental leaks of sensitive data. Think of malicious or unwitting employees misusing classified data by sending classified emails to the wrong user or taking home a flash drive containing classified data. Most government agencies are taking more preventative efforts to guard against this type of data loss. Seventy-five percent of respondents said their agency controls removable media to guard against such cases of data loss. (See Figure 7).

With DLP encryption capabilities, you can also ensure that technologies are built to protect individuals' privacy.

The reasons to implement the CSF's Protect function and deploy DLP are highly compelling. It's helpful, however, to know common challenges that agencies encounter when trying to do so because the benefits of the Protect function and DLP far outweigh potential barriers.

FIGURE 5

Does your agency use data loss prevention tools to control what data end users can transfer or share outside of your agency's network?

FIGURE 6

If yes, do the data loss prevention tools protect sensitive and high-value data on-premise and in the cloud?

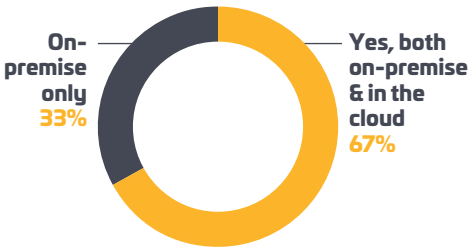


FIGURE 7

Does your agency control removable media to guard against data loss?

Challenges to Protection & Data Loss Prevention

It is likely no surprise that deploying DLP may be easier said than done. There are many cybersecurity priorities to focus on, and shelving the wrong ones could result in serious damage to critical infrastructure. Then, there's the added challenge of figuring out what data your agency must protect and where it is located. Compounding the problem is the shortage of the skilled IT workforce you need to help tackle these issues. Together, these pose significant challenges to DLP and implementing the CSF's Protect function.

Our survey respondents cited competing cybersecurity priorities (27 percent) as the biggest obstacle to DLP deployment, followed closely by identifying data location and data workflows (21 percent) and lack of trained personnel (21 percent). (See Figure 8).

FIGURE 8

Whether or not your organization is implementing DLP, what is the biggest obstacle to DLP deployment?

1. Competing Cybersecurity Priorities

Whether it's identifying your agency's cyber risks, protecting assets or simply navigating the many regulations and frameworks the government must comply with, multiple cybersecurity priorities could hold equal importance. The challenge is, on which do you focus?

For instance, implementing the CSF's guidelines when there are other mandates to comply with, including NIST's Risk Management Framework, the Federal Information Security Management Act (FISMA) and/or the Federal IT Acquisition Reform Act, can be tough. "Many agencies view the CSF as an added level of bureaucracy on top of the risk management framework," Durbin said.

There are also increasingly more devices and apps to monitor that contain critical information to protect. For example, a health agency has 220,000 makes and models of devices to track, Maclean said. Those high-value assets have an impact not just on the agency's work, but also someone's health and livelihood.

When cybersecurity gets too complicated, it becomes difficult to account for costs and alignment with your agency's mission. But by using the guidelines under the Protect function of the CSF, you can better align cybersecurity priorities such as identity and access management, data classification and personnel training.

2. Identifying Data Location and Workflows

Another challenge to DLP and protecting your agency's high-value assets can be knowing what data you have and where it's located. "For many agencies, the difficult part is simply identifying them," Durbin said. "It's harder than you might expect to know where your data actually is or what your assets actually are."

Even if your agency has decided to deploy DLP, it's hard to get started without knowing what data to incorporate into the tools and solutions. "Identifying data is time consuming and data often isn't centrally located," DLT's Maclean said.

As new technologies and platforms develop, your agency will need to constantly reassess its technology to ensure it can still combat new and evolving threats. But not only must your technology and staff be equipped to deal with cyberthreats, they must also be equipped to track your data and who's accessing it so they can mitigate cyberattacks.

FIGURE 9

The CSF "Protect" function also focuses on addressing "Awareness and Training" for end users. Do you think your agency's users are adequately trained and security-aware?

3. Lack of Trained Personnel

It is well known that one of the biggest hindrances to enhancing the government's cyber posture is the lack of cybersecurity training within the current workforce and qualified candidates to recruit. Although the challenges in the cyber workforce are very real, the perception that agencies are lagging may be worse than the reality.

When asked if they thought their agency's users are adequately trained and security-aware, 52 percent of survey respondents replied, "Yes." (See Figure 9). However, at the same time, respondents cited lack of trained personnel as one of the biggest challenges to DLP deployment.

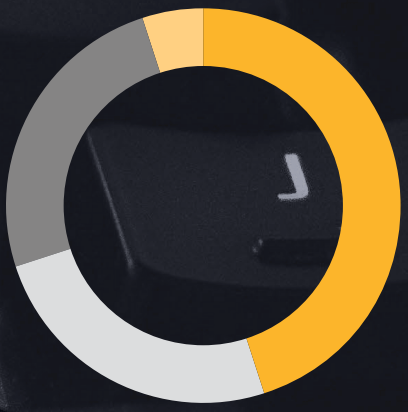
Maclean attributed the personnel issues to constraints of government contracting vehicles. "In addition to trying to write contracts that seek people with the appropriate level of training, it's also important to keep the contract as stable as possible," Maclean said. "Under the terms of a government contract, contractors don't get to take time off for training. Facilitating training, however, pays off in the long run. It not only gives you better-trained personnel, but also enhances workforce stability because they want to stick around."

Durbin believes many government employees are more aware than they think, especially when they focus on the Protect function of the CSF. "If they focus on how the Protect function lines up with what they're already doing (i.e., FISMA), they're more likely to satisfy the Protect function," he said. "They just might not see it that way, so many feel they're not adequately trained."

Using the CSF's Protect Function to Improve Security

Although you may face significant barriers to DLP deployment and protecting your most high-value assets, there are ways you can use the CSF to improve your agency's cybersecurity. Maclean and Durbin outlined three steps agencies can take to make the most out of DLP and the CSF Protect function.

FIGURE 10
Is your agency planning to deploy a data loss prevention tool?



- **No plan 45%**
- **Yes, this fiscal year 25%**
- **We are waiting for the Continuous Diagnostics and Mitigation program to address data protection 25%**
- **Yes, next fiscal year 5%**

"The bottom line is you need to make sure you have visibility over where your data is, where it's going and can protect it even if it's encrypted."

KEN DURBIN
CISSP Senior Strategist of Global Government Affairs and Cybersecurity at Symantec

1. Identify Your Data

You may need to start with the CSF's Identify function to develop the organizational understanding to manage cybersecurity risks, systems, assets, data and capabilities. The Identify function helps you know where all your assets are so that you can use your DLP solution and the Protect function to know where to look for and classify data.

The Identify function can also help ensure that you look at every component of your cybersecurity approach, including expertise, networks, servers and assets. Durbin suggested using solutions within your DLP to help automate the process. "You can automate not just the identifying of data, but also the classification," he said.

You can do this using either a prebuilt template or teaching the DLP system through machine learning to identify sensitive data and classify it appropriately. You can then meet Identify function requirements, such as establishing mitigation priorities through automation and developing reliable and reproducible processes.

Maclean also suggested using a diagram to better track your agency's data. "Identify not just where your data is statically, but also what are the sanctioned data flows, particularly if you're sharing it with another agency."

2. Extend Identity & Access Management into the Cloud

The CSF Protect function specifically supports the ability to contain the impact of a potential cybersecurity event through access control and data security. This is particularly useful if your agency is not ready to implement full-on DLP just yet. Start by identifying your agency's users, credentialing them and implementing access management. Out of survey respondents who have yet to deploy DLP, 45 percent said they have no plan in place, while another 25 percent are waiting for Continuous Diagnostics and Mitigation (CDM) to address it. (See Figure 10).

But Durbin and Maclean advised that you don't have to wait on CDM to start addressing identity and access management.

At the very least, begin enhancing the credentialing process for those using your agency's data. "Make sure there's two-factor authentication in place so you can at least ensure that the person trying to access the data is who they say they are," Durbin said. He also suggested using encryption for those who do not have access to the data. "If somebody does get access to data that they're not supposed to, it's harder for them to do something bad with that data."

Even if your agency may not quite be ready for DLP, you can still stay ahead of cyberthreats through other means and add protection to your high value assets. These can include identity and access management. With those, you can attain enhanced control, convenience and compliance in protecting your agency's most high-value assets.

3. Extend the Visibility of Your Data Protection Solution

The CSF Protect function provides guidelines on security awareness and training. But no matter how good your IT or cybersecurity teams are, it's always helpful to have the right technology tools at your disposal. Fortunately, the Protect function also provides guidelines for investing in protective technology. Additionally, Durbin and Maclean suggested extending the visibility of your DLP solution so you can protect your data whether it's on premise or in the cloud, even if encrypted.

"Symantec's DLP solution, combined with our CASB/CloudSoc, allows you to extend your existing DLP policies and workflows into the cloud to help prevent data loss through SaaS Apps. DLP also protects cloud-based email with our Email Security Service, and even encrypted traffic with our Web Security Service Proxy," Durbin said. "The bottom line is you need to make sure you have visibility over where your data is, where it's going and can protect it even if it's encrypted."

Your visibility solution ideally should be on a unified platform that allows you to see your data through a single console, identify data that's classified and data that's not and prioritize and remediate cyber threats across multiple control points.

How Symantec & DLT Can Help

To use the three best practices while taking advantage of all the CSF has to offer, you can turn to leading experts in the federal community, Symantec and DLT. Both companies are tuned into the cyber priorities of government and how they're being measured.

"We understand the existing architecture, the move to the NIST Cybersecurity Framework and how cloud-enabled solutions can help," Durbin said. "We can position our solution to help line up with those priorities and frameworks."

For example, Symantec's DLP solution is already mapped to the CSF, so your agency can deploy DLP assured that it will help you stay compliant and protect your data. A key benefit of Symantec's DLP is discovering where your data is stored across all your cloud, mobile, network, endpoint and storage systems. Additionally, you can monitor how employees use data both on and off the network while protecting it from being leaked or stolen.

DLT is also partnering with Symantec to offer even more comprehensive cybersecurity solutions so that your agency can comply with utilizing the CSF and many other important regulations.

DLT and Symantec work together to provide your agency with data protection, cybersecurity and threat-protection software solutions. They strive to ensure that agencies can better correlate all gathered security data and more effectively prioritize and focus mission efforts. They help agencies identify their data and workflows, prioritize identity access and management, and deploy DLP solutions in holistic platforms that provide utmost visibility.

Conclusion

To best protect your agency's most critical assets while ensuring that your data is safe, you will need to continue investing in data loss prevention and identity and access management in addition to training and educating the cyber workforce of tomorrow. These efforts can be enhanced with the right solutions, encompassing DLP and a way to automate the protection of your agency's most valuable information.

Symantec and DLT can help you effectively discover what is on your network and continuously assess and manage your cyber posture, all while making the most out of the NIST Cybersecurity Framework.

About Symantec

Symantec helps federal agencies develop and implement comprehensive and resilient security strategies to reduce risk and meet Cross-Agency Priority Goals, the NIST Cybersecurity Framework, the Joint Information Environment and other federal mandates.

Learn more at: **www.symantec.com.**

About DLT

For 25 years, DLT Solutions has been dedicated to solving public sector IT challenges.Guided by our relentless focus, we have grown to be one of the nation's top providers of world-class IT solutions. Leveraging our strategic partnerships with top IT companies, we develop best-fit solutions for our customers. Our sales, integration, and support experts have the certifications and experience in helping customers at any level of any agency. We have both deep subject matter expertise and in-depth knowledge of government mandated requirements and initiatives in areas such as a cloud computing, cybersecurity, and consolidation.

Learn more at: **www.dlt.com.**

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 270,000 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 **info@govloop.com**.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop