Achieving Successful Outcomes With the NIST Cybersecurity Framework

Cyberattacks are a serious threat to our economy and national security. Government agencies at all levels need to be able to detect, defend and respond to threats.

To address the growing cyber risk, the National Institute of Standards and Technology (NIST), in partnership with private sector industry, developed the Cybersecurity Framework (CSF), which provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes.

To learn more about the CSF's usage, perception and outcomes in government, particularly its five functions, GovLoop teamed with Symantec, a leader in cybersecurity, to survey groups of federal employees. Read on below for statistics, challenges, and how CSF is being used in government at the federal, state and local level.

Per the Executive Order on Cybersecurity, have you started implementing the CSF?

61% YES 39% NO

Have you implemented all of the CSF's recommendations or just some?

39% ALL 60% SOME 1% NONE

What is your confidence level in the CSF to improve your agency's cybersecurity posture?

68% HIGH 30% MED 2% LOW

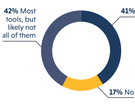
Identify

This function calls on organizations to look at every component of their cybersecurity enterprise. That includes hard security assets, such as servers and networks, as well as soft assets, such as software, data and people. It also addresses concerns like governance, risk management approach and business use.

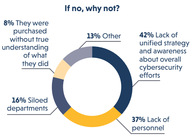
Has your agency explored the Identify function of the CSF?

91% Yes

Is your agency fully aware of all procured cybersecurity tools at their disposal?



If no, why not?



TAKEAWAY

You can't protect what you can't see. Identify and manage all of your hardware and software assets with Symantec's **IT Management Suite**.

Protect

The goal of the Protect function is to develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. The Protect function supports the ability to block attacks where possible.

Has your agency explored the Protect function of the CSF?

93% Yes

The 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?

52% Yes

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

70% Yes

TAKEAWAY

Your systems and their data must be secured, no matter where it lives. Symantec's **CASB solution** and **Data Loss Prevention** suite of tools help you protect your data, whether it is on-premise or in the cloud.

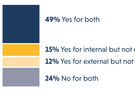
Detect

The Detect function defines the appropriate activities to identify the occurrence of a cybersecurity event, and enables timely discovery of cybersecurity events.

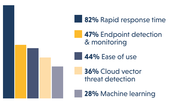
Does your agency comply with or follow the Detect function of the CSF?

77% Yes

Do you feel your agency's current detection capabilities are adequate for both external and internal threats?



What abilities are most critical to you in a detection solution? Check your top 3.



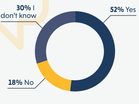
TAKEAWAY

You need to know when an attack or breach occurs, as soon as it happens, in order to react and minimize damage. Symantec's **Endpoint Detection and Response** solution can detect security events in real time and alert your team.

Respond

The Respond function includes appropriate activities to take action regarding a detected cybersecurity incident, and supports the ability to contain the impact of a potential cybersecurity incident.

Do you have a response plan for cyberattacks in place at your agency?



If no, what's preventing your organization from implementing a response plan?

Do you feel you have the proper technologies in place at your agency to respond to attacks?

61% Yes

TAKEAWAY

The difference between a security event and a breach is the ability to quickly take action. Symantec can help agencies respond to security alerts and incidents, as well as minimize the impact of cyber attacks, with their **Managed Security Services**.

Recover

The Recover function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident, and supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

Does your department have a recovery plan for cyberattacks in place?

If no, what's the biggest reason preventing your organization from having one?

Was your recovery plan useful?

100% Definitely or somewhat useful

TAKEAWAY

When breaches occur, agencies must be able to quickly recover their data and get systems back online. Symantec's **Incident Response Services** can assist with fast threat containment and eradication, as well as prepare and test the efficacy of agency incident response plans.

Having a cyber framework in place yields many benefits for agencies, particularly in knowing where to start combating cyberthreats or implementing recommendations. While following NIST's recommendations does not necessarily guarantee elimination of cyberthreats, it will significantly improve overall cybersecurity posture at all levels of government.

Symantec can help your agency with data protection, cybersecurity and threat-protection software solutions. They help agencies understand the CSF and how it can benefit them – and their holistic solutions map to each of the five functions.

Learn more about Symantec's solutions for state & local government

Learn more about Symantec's solutions for federal government

Symantec. govloop