Achieving Successful Outcomes With the NIST Cybersecurity Framework

Cybersecurity is 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 this pressing issue, the National Institute of Standards and Technology (NIST) coauthored a report in January 2013 with private sector leaders to develop the Cybersecurity Framework (CSF). The NIST Cybersecurity Framework is a set of principles, practices and guidelines to help organizations determine what cybersecurity strategies and tools are appropriate for their environment.

To support the implementation of the CSF, NIST developed an electronic version of the CSF to help the federal, state and local governments adopt CSF-based practices. Based on the NIST Cybersecurity Framework, Symantec can help your agency with data protection, cybersecurity and IT Management Suite.

### Identify

The NIST Cybersecurity Framework identifies five functions to help organizations manage cybersecurity risks. The Identify function of the CSF addresses “Threat Management” for end users. The Identify function also addresses concerns like governance, risk management approach and business use.

**TAKEAWAY**

If yes, explain why you selected the identified solution?

91% Yes

### Protect

The goal of the Protect function is to develop and implement appropriate safeguards to ensure delivery of normal operations to reduce the impact from a cybersecurity incident. The Protect function supports the ability to block attacks where possible.

**TAKEAWAY**

If yes, explain why you selected the identified solution?

93% Yes

### Detect

The Detect function defines the appropriate activities to identify the occurrence of a cybersecurity event, and minimize recovery of cybersecurity outcomes.

**TAKEAWAY**

If yes, explain why you selected the identified solution?

77% Yes

### Respond

The Respond function includes appropriate activities to take action regarding a detected cybersecurity event. The Respond function also focuses on “Awareness and Training” for end users.

**TAKEAWAY**

If yes, explain why you selected the identified solution?

61% Yes

### Recover

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

**TAKEAWAY**

If yes, explain why you selected the identified solution?

100% Definitely or somewhat useful

Having a plan in place to protect your business is important for agencies, particularly for nonprofits that are not equipped to handle cybersecurity threats. Symantec can help agencies protect their data and prevent attacks with threat management, as well as support recovery to reduce the impact from a cybersecurity event.

### Statistical Analysis

- 61% of respondents have a plan in place to protect your business.
- 93% of respondents have a plan in place to protect your business.
- 77% of respondents have a plan in place to protect your business.
- 61% of respondents have a plan in place to protect your business.
- 100% of respondents have a plan in place to protect your business.

### Further Reading

For more information on Symantec’s solutions for federal & local government, visit [Symantec’s website](https://www.symantec.com).