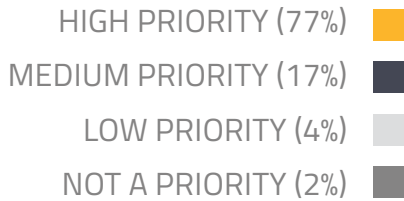
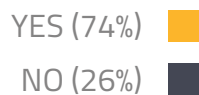


Government Perceptions of the NIST Cybersecurity Framework

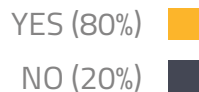
What priority is cybersecurity at your agency?



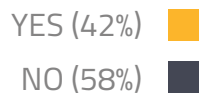
Will your agency invest more resources (money, staff, etc.) in cybersecurity efforts in 2017?



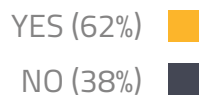
Does your agency leverage a security framework?



Do you know what the NIST Cybersecurity Framework is?



Does your agency leverage the NIST Cybersecurity Framework?



The NIST Cybersecurity Framework, which was created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure and improve government cybersecurity. GovLoop partnered with Symantec, an industry leader in cybersecurity solutions, for this survey of 284 public sector employees about the Framework's usage, perception, and outcomes in government.

Cybersecurity remains a massive priority across government agencies. In fact, a high number of respondents (77 percent) said cybersecurity is a top priority at their agency.




This is reflected in the additional fact that most respondents (74 percent) said their agencies plan on investing more resources (money, staff, etc.) in cybersecurity efforts in 2017 than the previous year.

Additionally, most respondents (77 percent) said their agency already leverages some sort of security framework.

Of those respondents who do not leverage a cybersecurity framework already, half (58 percent) said that they did not know what the NIST Cybersecurity Framework was, reflecting a possible lack of information of education around the availability of the NIST Framework.



But in news that points towards a good adoption trend of those in the know about cybersecurity frameworks, of those survey respondents whose agencies do employ a framework, 62 percent said the framework they use is the NIST Cybersecurity Framework. ►

Have you implemented all of the NIST Cybersecurity Framework's recommendations or just some?

ALL (39%) 
SOME (60%) 
NONE (1%) 






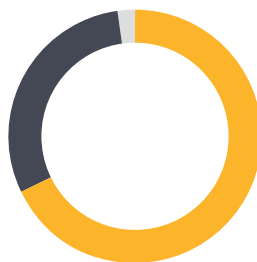
Does your agency plan to implement the NIST Cybersecurity Framework in the next 12 months?

YES (38%) 
NO (62%) 





What is your confidence level in the NIST Cybersecurity Framework to improve your agency's cybersecurity posture?

HIGH (68%) 
MEDIUM (30%) 
LOW (2%) 



Do you believe that using the Framework has reduced or will reduce your cybersecurity risk?

YES (85%) 
NO (15%) 



But there's work yet to be done. Of the respondents who do use the NIST Cybersecurity Framework, only 39 percent have implemented all of the recommendations. 60 percent have implemented just some of the recommendations, and 1 percent said they have not yet implemented any of the recommendations of the Framework.

There also needs to be a push for adoption in agencies who have not yet implemented the Framework. Only 38 percent of respondents who do not yet follow the Framework say their agencies do plan to implement it in the next 12 months.

But though there is some need on the education, awareness, and implementation front of the NIST Cybersecurity Framework, the good news is that those who do use it have clearly seen the benefits.

When asked, "What is your confidence level in the NIST Cybersecurity Framework to improve your agency's cybersecurity posture?" the majority of respondents (68 percent) said their confidence levels were high.

Most importantly of all, faith of survey respondents in the Framework helping their cybersecurity efforts is high – 85 percent believe that using the Framework has reduced or will reduce their cybersecurity risk.

Now the question for government and NIST becomes: how do we get more agencies adopting the Framework, and how do we continue our education and sharing of best practices?

Visit govloop.com for more information and to sign up for an upcoming research brief that will explore this topic.

