

What is a framework?

Name: Melvin Orienza


Date: 09/08/2019

Details

A framework is a document containing a set of guidelines that an organization compares its standards against. Another way to describe a framework is a collection of best practices. Frameworks can give us a look at the bigger picture. They try to address issues an organization may face. Organizations also have to take the framework into account when making financial decisions. It should be acknowledged that while all may benefit from a framework, every organization's situation is not the same. The framework is not meant to be used as the immediate solution but rather to supplement what is already going on (U.S. Department of Commerce, 2018, p. 13).

Taking cybersecurity into account, all of these ideas are very important. The NIST is one of the frameworks used when talking about cybersecurity, This one was worked on collaboratively so many perspectives have been put into it (U.S. Department of Commerce, 2018, p. iv). With technology being rapidly implemented into our society, the importance of companies keeping their cybersecurity up is increasing. Failing to do so can result in serious losses for those who work in the organization and those they serve as well. Data can be lost if a cybersecurity attack happens which means the affected group can potentially lose money, reputation, and operational time to name a few things. Taking the NIST's information into consideration is something every business should do.

The NIST Framework is defined by five core activities. The identify activity is done to make known what needs to be protected and what the organization is currently able to do to achieve that. Protect means to create solutions and use them to defend what keeps the company going (or in other words, what was identified).



The detect part of the core is putting measures in place to make sure that when a cyber attack happens, the business is aware of the attack as soon as possible (U.S. Department of Commerce, 2018, p. 7). Respond is the part of the core involving the actions taken when a cyber threat occurs. The recover function aims to maintain the operational status of an organization or bring it back up when an attack occurs (U.S. Department of Commerce, 2018, p. 8). All organizations conduct these five functions to keep their organization going.



References

U.S. Department of Commerce, National Institute of Standards and Technology (2018),
Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). Retrieved from:
<http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>