

NIST Cybersecurity Framework

Name: Mina Adams

Date: January 27, 2020

Details

Cybersecurity is the glue that holds the internet together. Without it, the internet and everyone's data would be up in flames, most likely literally and figuratively. It is taken for granted each day by the everyday user, because most people do not quite realize the urgency that comes with good cybersecurity practices and how it benefits them.

A framework is an extremely vital facet of any operating system, business, et cetera. It is essentially a game plan for cybersecurity that is used by many different people involved within the system. It is imperative that all possible threats and exploits are taken into account, and that risk is readily assessed. With a framework, all of this and more is used in tandem in order to protect anything necessary. Frameworks benefit all sides of the exchange, like the user, the business, and the actual infrastructure itself. According to NIST, "the Framework includes a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities."

There are five key activities associated with said framework. The goals of the framework are to describe a system's current structure on cybersecurity, to describe their target or goal state of their cybersecurity, to identify the opportunities and the processes associated with reaching their targeted state of improvement, take into account the current progress they are making and the procedures they are putting into place, and to use the framework to communicate to businesses outside and people within the business about their threats and exploits.

References

Introduction. (n.d.). *NIST Cybersecurity Framework*, 8–16. doi: 10.2307/j.ctv4cbhfx.4