The NIST Cybersecurity Framework

Having a plan is just one part of securing assets.
Once the plan is in action, the other part is making sure everyone's following along.
In security, we call this compliance.

Compliance is the process of adhering to internal standards and external regulations.
Small companies and large organizations around the world place security compliance at the top of their list of priorities.
At a high-level, maintaining trust, reputation, safety, and the integrity of your data are just a few reasons to be concerned about compliance.
Fines, penalties, and lawsuits are other reasons.
This is particularly true for companies in highly regulated industries, like health care, energy, and finance.
Being out of compliance with a regulation can cause long lasting financial and reputational effects that can seriously impact a business.

Regulations are rules set by a government or other authority to control the way something is done.
Like policies, regulations exist to protect people and their information, but on a larger scale.
Compliance can be a complex process because of the many regulations that exist all around the world.
For our purpose, we're going to focus on a framework of security compliance, the U.S. based NIST Cybersecurity Framework.

Earlier in the program, you learned the National Institute of Standards and Technology, or NIST.
One of the primary roles of NIST is to openly provide companies with a set of frameworks and security standards that reflect key security related regulations.
The NIST Cybersecurity Framework is a voluntary framework that consists of standards, guidelines, and best practices
to manage cybersecurity risk. Commonly known as the CSF, this framework was developed to help businesses secure one of their most important assets, information.
The CSF consists of three main components: the core, it's tiers, and it's profiles.
Let's explore each of these together to build a better understanding of how NIST's CSF is used.

The core is basically a simplified version of the functions, or duties, of a security plan.
The CSF core identifies five broad functions:
identify, protect, detect, respond, and recover.
Think of these categories of the core as a security checklist.

After the core, the next NIST component we'll discuss is its tiers.

These provide security teams with a way to measure performance across each of the five functions of the core.
Tiers range from Level-1 to Level-4.
Level-1, or passive, indicates a function is reaching bare minimum standards.
Level-4, or adaptive, is an indication that a function is being performed at an exemplary standard.
You may have noticed that CSF tiers aren't a yes or no proposition; instead, there's a range of values.
That's because tiers are designed as a way of showing organizations what is and isn't working with their security plans.

Lastly, profiles are the final component of CSF.
These provide insight into the current state of a security plan.
One way to think of profiles is like photos capturing a moment in time.
Comparing photos of the same subject taken at different times can provide useful insights.
For example, without these photos, you might not notice how this tree has changed.
It's the same with NIST profiles.

Good security practice is about more than avoiding fines and attacks.
It demonstrates that you care about people and their information.
Before we go, let's visit the core's functions one more time to look at where we've been and where we're going.
The first function is identify. Our previous discussions on asset management and risk assessment relates to that function.
Coming up, we're going to focus on many of the categories of the second function, the protect function. Meet you there!

Revision #1
Created 2023-07-17 23:52:02 UTC by naruzkurai
Updated 2023-08-15 18:44:10 UTC by naruzkurai