The NIST Cybersecurity Framework

The NIST Cybersecurity Framework is an excellent tool that organizations can use to establish or improve their cybersecurity position. This framework is comprehensive and flexible, allowing organizations to tailor it to their specific needs. The framework includes five core functions: Identify, Protect, Detect, Respond, and Recover. Each of these functions includes a set of categories that an organization can use to assess their current readiness and identify areas where improvements can be made. This can help a company have an easier time complying with any laws or regulations that they need to as they can determine what areas are lacking and focus on them. There is also the benefit that a framework such as this makes it easier for different organizations to communicate with each other about cybersecurity related matters as everyone is on the same page. How this framework can be used in a workplace largely depends on the industry. For example, in the financial or retail industries, the framework can be used to implement security controls and detect threats to protect customer information and prevent fraud. In the industrial sector, it can be used to identify assets and systems that are considered critical and implement ways to protect them from various cyber threats.

1. Identify	Understand and manage cybersecurity risks to systems and organizational assets
2. Protect	Implement safeguards and secure data to protect against potential threats
3. Detect	Develop and implement activities to identify cybersecurity events in a timely manner
4. Respond	Establish and execute an effective response and recovery plan to mitigate the impact of incidents
5. Recover	Develop and implement activities to restore normal operations and services after an incident

The CIA Triad

The CIA triad is a model that organizations use as a guide to tailor their cybersecurity policy. (Chai, 2022) The CIA acronym stands for confidentiality, integrity, and availability. These three concepts are considered foundational to information security and should always be considered. The triad aids organizations in evaluating their current products or policies to determine how value is being offered in these key areas.

Confidentiality

Confidentiality refers to the goal of keeping data private. Measures in this area are created to prevent unauthorized persons from accessing private information. Organizations can improve their standing in this area by providing personnel with access to sensitive information special training for handling data of this kind to ensure confidentiality. (Chai, 2022) They can also utilize techniques such as data encryption and two-factor authentication.

Integrity

Integrity is concerned with making sure that data is accurate and untampered with. It is important to make sure data is not manipulated while in transit by a hacker using techniques such as a Man in the Middle attack. There are multiple ways for an organization to improve in this area. Not all risks related to data integrity can be attributed to nefarious cybercriminals. Even cosmic rays can pose a threat to data integrity as they can cause bit flips that can change or corrupt data. (Ferreira, 2017) It is important for any organization storing data to make sure the data is backed up properly and restorable in any event.

Availability

This area of the triad represents the need to ensure that data is always available to be accessed by the authorized parties. The best way to ensure compliance with this area of the triad is to maintain all hardware and keep all systems updated regularly. (Chai, 2022) Storing proper backups is important in this area as well, as a quick, efficient disaster recovery plan is integral to data availability.

Authentication vs. Authorization

While similar, authentication and authorization are two different concepts in computer security. They both deal with determining the identity of a user and what they are allowed to access. Authentication is the process of verifying the identity of a user. Authorization is the proves of granting or denying access based on the authenticated identity of the user. A good example of this is the use of a keycard.

Opportunities for Workplace Deviance

For years now, advances in cyber technology have allowed organizations to increase productivity and conduct business easier than ever before. Unfortunately, these advances do not come without their own drawbacks and concerns. Along with increased opportunity for productivity gains, cyber advancements have also brought about many opportunities for employees to engage in various forms of workplace deviance. Workplace deviance refers to voluntary and intentional behavior that violates organizational norms and ethics. Workplace deviance can take many forms, such as theft, sabotage, cyber misconduct, among many others. Amidst the ever-growing risks faced by organizations today, the possibility of employees carrying out cyber attacks for personal gain or revenge after being terminated looms large as a major concern. For example, e-mail has become integral to many organizations around the world but can easily be used by someone to run a phishing scheme on customers or fellow employees using organizational credentials. Electronic databases provide an easy and efficient way for a company to store information, but it can also be a tool for an employee, disgruntled or otherwise, to obtain confidential information. One example of this occurred in 2015 when a Morgan Stanley employee was fired for stealing account information on over 300,000 financial clients. (Baer, 2015)