Describe one of the five principles of the NIST Cybersecurity Framework and how organizations can apply them to their cybersecurity programs.

NIST developed the NIST Cybersecurity Framework as a voluntary Cybersecurity Framework for operators of critical infrastructure. The framework was developed after NIST got directed by Executive order. The order was concerned about the cybersecurity of critical infrastructure that encourages efficiency, innovation, and prosperity while promoting security, confidentiality, privacy, and civil liberties (Kosseff, 2017). The Cybersecurity Framework draws upon existing security practices, and It's not a one-size-fits-all framework. Instead, companies determine the set of activities that are essential to critical service delivery and prioritize investments to maximize the impact of the money they spend (Kosseff, 2017). With that being said, many firms, large and small, are adopting the framework. The NIST Cybersecurity Framework consists of five key principles that organizations need to focus on when designing their security policies. These principles include identity, protect, detect, respond, and recover.

Specifically, the protect principle is concerned with developing and implementing appropriate safeguards to ensure the delivery of services. Organizations can apply this core principle to their cybersecurity programs by examining several categories and developing rigorous mechanisms to execute them. The categories include

* Access control: limiting access to assets and facilities to authorized users, process, or devices, and to authorized activities and transactions.
* Protective Technology: Deploying technical security solutions such as DLP to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
* Information Protection Processes and Procedures: Developing security policies (addressing roles, responsibilities, management commitment, and coordination among organizational entities) and procedures to manage the protection of systems and assets.
* Awareness and training: Providing employees and the organization’s partners cybersecurity awareness educations and adequately training security individuals with information related to their duties and responsibilities.
* Data Security: Managing information and records with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.
* Maintenance: Maintaining and repairing industrial control and information system components is performed consistent with policies and procedures (“NIST Special Publication 800-53 Revision 5, Security and Privacy Controls…”, 2017).

Reference

NIST Special Publication 800-53 Revision 5. *Security and Privacy Control for Federal Information Systems and Organizations*. (2017). Retrieved from: https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

Kosseff, J. (2017). *Cybersecurity Law.* Hoboken, N.J: John Wiley & Sons, Inc.