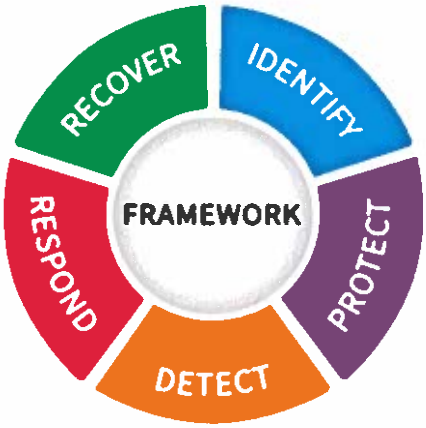
Fact Sheet
Information Technology Security

CYBERSECURITY AWARENESS

National Institute of Standards & Technology – NIST Cybersecurity Framework – CSF[123]

By Dr. Angel Hueca CPP, Jim Hannigan, Rex Lam CPP



What It Is

- Voluntary guidance based on existing standards, guidelines and practices
- Helps organizations better manage and reduce cybersecurity risks
- Integrate and align cybersecurity risk management with the broader enterprise risk management
- The CSF does not prescribe any particular specific technical activities or solutions. Rather it lays out concepts and policy-like ideas to facilitate an awareness, a mindfulness

How It Works

Organized into 5 Key Functions

- These functions and associated operations and activities do not require an in-depth understanding of IT.
- They follow the traditional, standard approach to risk management across the board.
- They can be implemented by Non-Cybersecurity and even Non-Security professionals.

[1] https://www.nist.gov/cyberframework
[2] https://csrc.nist.gov/publications/detail/nistir/8286/final
[3] https://verveindustrial.com/resources/case-study/achieving-nist-csf-maturity-with-verve-security-center/

The ASIS IT Security Steering Committee created this resource for the ASIS Global IT Security Community.
Originally published: 11 October 2021

These five Key Functions are graphically detailed below.

Identify

Develop an organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities. Having an asset inventory will assist you in better understanding your network and where critical data and pressure points may be.

Protect

Develop and implement the appropriate safeguards to ensure delivery of services. Managing access to assets and information, protecting sensitive data, authenticating users and implementing integrity checks all contribute to this protection.

Detect

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. In cases where protection is somehow bypassed or rendered ineffective processes such as regular back-ups and installing firewalls help to mitigate and reduce the impact. Understanding the normal flow of data and information throughout the organization helps to recognize unusual and perhaps malevolent occurrences.

Respond

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. Since threat actors constantly revise their attack vectors and methods it is imperative to test and update the defensive postures and responses in place.

Recover

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. A great deal of communication and coordination is required for Recovery. The internal and external stakeholders must be kept informed on the status of the problem and damage, as well as of the Response solutions. Equally important on a corporate level is communication with general public to maintain the company's reputation.