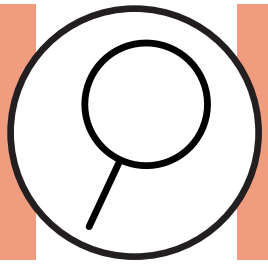
Demystifying NIST Cybersecurity Framework

Initially developed for critical infrastructure, the **National Institute of Standards and Technology (NIST)** established a framework for improving cybersecurity, titled the NIST Cybersecurity Framework.

At the core of the framework exists five functions, which are further divided into multiple categories and subcategories, providing a roadmap to help organizations strengthen their defense against cyberthreats. It's not compliance–it's a customizable strategy that can be applied to existing security programs, or used to build one from the ground up.

Identify

"Develop the organizational understanding to manage cybersecurity risks to people, systems, assets, data, and capabilities."



One of the most crucial steps to preventing cyberattacks is performing a risk assessment and identifying vulnerabilities. Organizations must review their assets and gain insight on how those assets might be valued by cybercriminals. By analyzing what you have and what you do, you can then identify vulnerabilities and focus your efforts from a top-down approach that fits business needs.

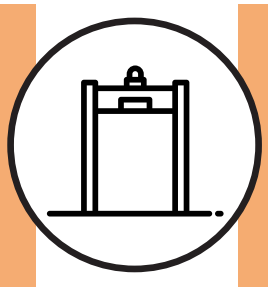
Protect

"Develop and implement the appropriate safeguards."

Protecting an organization starts with the people of the organization, which means implementing new-school awareness and compliance training, and developing stringent policies to mitigate risks. Protection also includes investing in security technologies (like threat detection services), and maintaining both hardware and software components so they never fall out of date, leaving them vulnerable to security holes.

Detect

"Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event."



Detecting threats in a timely manner is the difference between suffering a massive breach and eliminating the threat before it has a chance to do any real damage. To assist in this area, there are many software and hardware companies that offer services like real-time network monitoring, intrusion detection, phishing campaigns, etc. But this also comes down to a human issue in that employees need to stay alert and be on the lookout for potential attacks at all times.

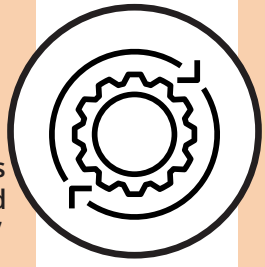
Respond

"Develop and implement the appropriate activities to take action regarding a detected cybersecurity event."

Any cybersecurity strategy is only as good as its incident response plan. Why? Because this is always a "when, not if" environment. Organizations need to have the proper procedures in place to help employees and team members quickly assess a potential attack, and know immediately how and where to report said attack. Think of it as an emergency plan that establishes a set of protocols—a step-by-step policy—to mitigate further damage and increase the success of recovery.

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."



Unfortunately, security events happen and they happen often. A strong recovery plan at least mitigates the fallout and helps to effectively restore systems and processes in a timely manner. It's also a chance to implement any lessons learned from the incident into awareness training, ultimately lowering the likelihood of similar incidents in the future.