NIST CYBERSECURITY FRAME WORK

Made by: Maor Pardilov

Guidance by: Lior Barash

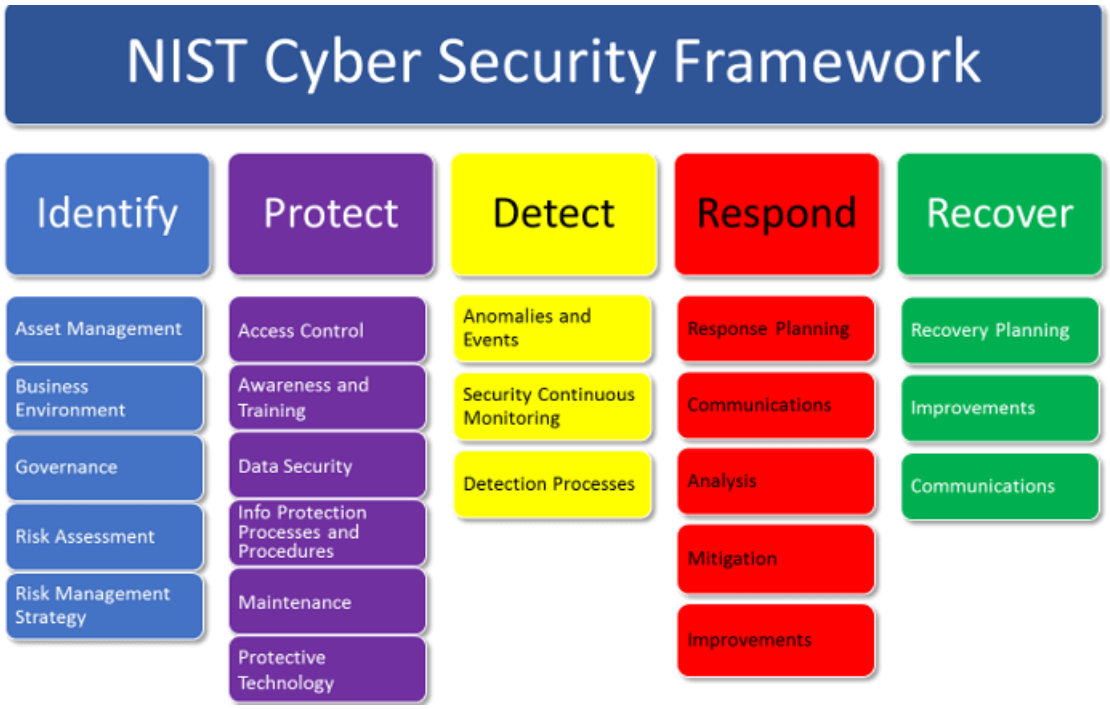
October 2020

Table of contents

1. Introduction....1
2. Identify....2
2.1 Asset Management -....2
2.2 Business Environment....2
2.3 Governance....2
2.4 Risk Assessment -....2
2.5 Risk Assessment Strategy -....2
3. Protect....3
3.1 Access Control -....3
3.2 Awareness and Training -....4
3.3 Data Security -....4
3.4 Info Protection, Processes & Procedures -....4
3.5 Maintenance -....4
3.6 Protective Technology -....4
4. Detect....5
4.1 Anomalies and Events -....5
4.2 Security Continuous Monitoring -....5
4.3 Detection Processes -....5
5. Respond....6
5.1 Response Planning -....6
5.2 Communications -....6
5.3 Analysis -....6
5.4 Mitigation -....6
5.5 Improvements -....6
6. Recover....6
6.1 Recovery planning -....6
6.2 Improvements -....6
6.3 Communications -....6
7. Summary and conclusions....7
8. Implementation NIST framework....7
8.1 diagram....7
8.2 Ransomware Risk Management....9

1. Introduction

The world we live in is a technological world. It's the truth. Cell phones, computers, Internet, social networks, online shopping, emails, cloud storage, money transfers through apps and much more. As more and more people use the internet our personal information is exposed as much as possible. This world includes endless information and unstoppable progress. Cyber-attacks for malicious purposes have become more and more common and nowadays every person who wants to protect his information and privacy or any company who wants to protect its assets and products needs an advanced and good defense system as possible. From a business point of view, every company wants to be the most advanced and first in its field. This desire includes a lot of risks and vulnerabilities and dangers in the network. Every company has assets and employees and sometimes a unique product that the company wants to maintain as much as possible. More than ever, organizations must balance a rapidly evolving cyber threat landscape against the need to fulfill business requirements. To help these organizations manage their cybersecurity risk, NIST convened stakeholders to develop a Cybersecurity Framework that addresses threats and supports business. The NIST cybersecurity framework is a powerful tool to organize and improve your cybersecurity program. It is a set of guidelines and best practices to help organizations build and improve their cybersecurity posture.



2. Identify

Identify - to recognize or establish as being a particular person or thing; verify the identity of.

2.1 Asset Management - asset management refers to the process of developing, operating, maintaining, and selling assets. Correctly identifying and in a cost-effective manner. Asset management is to know what is the value of the assets to the company and what impact it has.

2.2 Business Environment - sum or collection of all internal and external factors such as employees, customers needs and expectations, supply and demand, management, clients, suppliers, owners, activities by government, innovation in technology, social trends, market trends, economic changes, etc. what is the company business domain and what is the effect It has on the company.

2.3 Governance - standards and regulations. Governance has been defined to refer to structures and processes that are designed to ensure accountability, transparency, responsiveness, rule of law, stability, equity and inclusiveness, empowerment, and broad-based participation. forced on the company to respect and to stand on this standards and regulation because of the company domain.

2.4 Risk Assessment - Risk assessment is a term used to describe the overall process or method where you: Identify hazards and risk factors that have the potential to cause harm (hazard identification). What will be the damage if something will stop working or there will be a failure in the company system or service.

2.5 Risk Assessment Strategy - A strategic risk assessment is a systematic, continuous process for organizations to identify its strategic risks and understand how those risks are being managed across the business. What is the approach to get a solution? They entail the risk exposures that can ultimately impact on the services of the company or even threaten the business's survival. One of the most common strategies is the CIA triad.

CIA: Confidentiality, Integrity and Availability. The CIA Triad is actually a security model that has been developed to help people think about various parts of IT security.

Confidentiality - Confidentiality refers to an organization’s efforts to keep their data private or secret. Protecting confidentiality is dependent on being able to define and enforce certain access levels for information. In some cases, doing this involves separating information into various collections that are organized by who needs access to the information and how sensitive that information actually is - i.e. the amount of damage suffered if the confidentiality was breached. Some of the most common means used to manage confidentiality include access control lists, volume and file encryption, and Unix file permissions.

Integrity - Data integrity is what the "I" in CIA Triad stands for. This is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed.

Availability - This is the final component of the CIA Triad and refers to the actual availability of your data. Authentication mechanisms, access channels and systems all have to work properly for the information they protect and ensure it's available when it is needed. High availability systems are the computing resources that have architectures that are specifically designed to improve availability. Based on the specific HA system design, this may target hardware failures, upgrades or power outages to help improve availability, or it may manage several network connections to route around various network outages.

The identify category is the first category in this framework because every company must know and evaluate itself. Knowing what its work environment is, and evaluate its assets before it can even build a defense system. In order to protect yourself you need to know on what you are protecting.

3. Protect

Protect - to defend or guard from attack, invasion, loss, annoyance, insult, etc.; cover or shield from injury or danger. to guard (the industry or an industry of a nation) from foreign competition by imposing import duties.

3.1 Access Control - Access control is a fundamental component of data security that dictates who's allowed to access and use company information and resources. Through authentication and authorization, access control policies make sure users are who they say they are and that they have appropriate access to company data. Access control is an idea of protection. Almost every system has his own access control in his way and layer. **Every protection solution relies on access control.**

3.2 Awareness and Training - In cybersecurity, awareness training is a program designed to help users and employees understand the role they play in helping to combat information security breaches according to past cases. Awareness training helps employees to understand risks and identify potential attacks they may encounter. In addition, exposing employees to effective information that will help them protect the system and train them to work more efficiently.

3.3 Data Security - Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. It's a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures. Data security includes data encryption, hashing, tokenization, and key management practices that protect data across all applications and platforms.

3.4 Info Protection, Processes & Procedures - Information security policies and procedures are key management tools that assist in managing information security risk being faced by an organization. Information security policies and procedures of an organization should be in line with the specific information security risks being faced by the organization. Protecting valuable information such as passwords and usernames. Sensitivity and importance of information. The content of a file determines its level of importance. The more sensitive the information the file contains, the less exposure it will have to employees and only those with high sensitivity label will be able to access it. Sensitivity labels are used to add an additional layer of protection to your files or emails. They allow you to classify documents as confidential or highly confidential labels which once applied, determine what users can do with that file. Mandatory access control (MAC) is a security strategy that restricts the ability individual resource owners have to grant or deny access to resource objects in a file system. Each user and device on the system is assigned a similar classification and clearance level.

3.5 Maintenance - Security system maintenance. Control of laws and updates. Take care of system updates and protection updates on an ongoing basis. Perform a general update for all and not just for applications in particular. For example, checking permissions and tightening rules.

3.6 Protective Technology - These are technologies, tools and techniques to protect an individual or a community against things that would case it harm (hazards). What will be the technology that you will protect with? There are a number of products that will provide you with excellent protection on a variety of systems and networks. **Firewall** is the most common product that companies uses in order to monitor operations and protect the system in the best and most convenient way. **Firewall** is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls have been a first line of defense in network security for over 25 years. Firewall can be hardware, software, or both.

in conclusion, The Protect sector is the second category in this framework because after evaluating all our assets and our work environment in the last sector, now in this category we put the defensive idea into practice. Install protection products, perform access control and apply permissions to employees, perform updates and train employees to be prepared for attack situations, protect sensitive and insensitive information with the help of various protective equipment and products and emphasize the world of maintenance. The emphasis is on protection, how to protect the company and prevent attacks on our system and networks. Prevention of information theft and desire to grant permissions to users.

4. Detect

Detect - to identify, discover or discern.

4.1 Anomalies and Events - anomaly detection is the identification of rare items, events or observations which raise suspicions by differing significantly from the majority of the data. Typically, the anomalous items will translate to some kind of problem. Documenting events and identifying anomalies. Creating templates to build pattern rules. The event is making a pattern and the anomalies is showing the anomalies from order. Event Viewer is a tool in Windows that displays detailed information about significant events on your computer.

4.2 Security Continuous Monitoring - Continuous security monitoring (CSM) is a threat intelligence approach that automates the monitoring of information security controls, vulnerabilities, and other cyber threats to support organizational risk management decisions. A process that collects events and track them. Monitor almost anything that can be tracked. A utility program that reports the status of running programs. Task managers are used to review which applications and background processes are running, as well as to stop an app that is not responding. Wire Shark, N-Map, Elastic Search are great tools and programs that can help us monitoring.

4.3 Detection Processes - Processes that are performed in order to extract insights from operations that run on the monitor. Data analysis and all the events that run in monitoring.

To sum up, The Detect sector is the third category in this framework because in the previous category we focused on how to protect the system and what products to put and what technologies to use in order to provide our company with the best protection and highest efficiency when it comes to system updates. In this category we focus on identifying and monitoring and monitoring all network operations. Either I recognize the attack and block it or I block everything and allow specific things.

5. Respond

Respond - to reply or answer in words; to make a return by some action as if in answer.

5.1 Response Planning - Part of the response plan. How you want to react or how you react to an event together with the risk management strategy. Part of the protect design.

5.2 Communications - Communication inside and outside the company. In addition, the communication and connection between company employees and staff.

5.3 Analysis - Analyzing the event, understand what actually happened. incident response. Perform an investigation regarding the incident that occurred and be in control of what happened.

5.4 Mitigation - Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

5.5 Improvements - Perform improvement work after event detection. Response after an event immediately!

The Respond sector is the fourth category in this framework because in the previous categories we performed the installation of protective technology and the identification and monitoring of faults and problems, in this category we focus on our response plan to exceptional events and how we analyze them and how we act immediately to prevent them. In addition, emphasis is placed on communication between the company's employees and staff, as well as on external and internal communication. Furthermore, there is a focus on relief and improvement works in order to prevent and eradicate further intrusions and assaults.

6. Recover

Recover - to regain the strength, composure, balance, or the like, of (oneself); to regain health after being sick, wounded; to regain a former and better state or condition.

6.1 Recovery planning - Only when there is damage and need to recover and to get over from it. The day after. Planning a business continuity plan after a disaster or breach has occurred in the system. In addition, a disaster recovery plan if recovering. Backup! How to return to full function as before.

6.2 Improvements - Perform improvement work after event detection. Response after an event immediately!

6.3 Communications - Communication inside and outside the company. In addition, the communication and connection between company employees and staff.

The Recover sector is the last and final category in the NIST framework because in the previous categories we set up a comprehensive protection system for all our assets and systems, and in addition to all we installed monitoring and tracking systems for exceptional events and attacks on our system and network. In case our network is attacked or our internal system we will have to plan a way in which we can overcome everything and to plan a new business path and actually deal with the existing damage. How to return to full function like before. Of course it is important to remember to make a backup to all the data and systems we have in the company.

7. Summary and conclusions

After an in-depth review and analysis of the framework it can be concluded that the NIST cybersecurity framework is a powerful tool to organize and improve your cybersecurity program. It is a set of guidelines and best practices to help organizations build and improve their cybersecurity posture. The most important thing will be to follow the steps without skipping any of them.

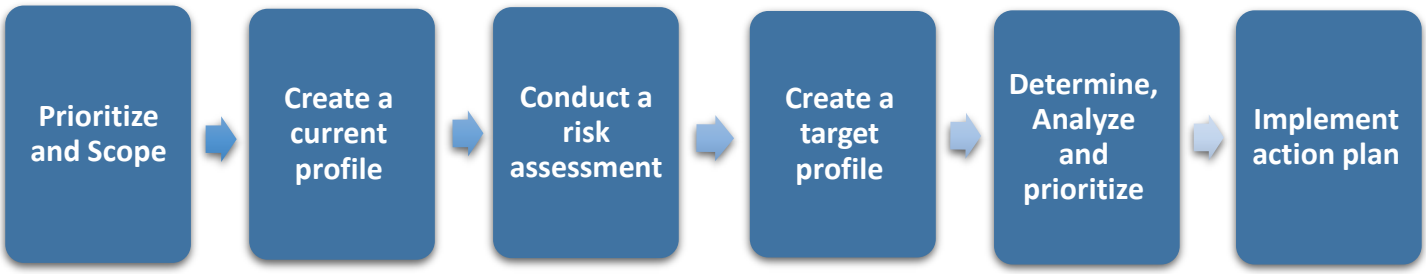
In the last years the NIST framework users base has grown to include communities and organizations across the globe. Based on a 2016 survey, 70% of respondents recognized NIST CSF as a popular security best practice.

You Have to Continuously Reassess How Much Risk Is Appropriate.

8. Implementation NIST framework

8.1 diagram

The following diagram is an example of implemented NIST farmeworker on business company.



Step 1: Prioritize and Scope

- Determine the scope to be addressed through the application of CSF. Is this organizational or partial?
- Identity organizational vision, mission, and strategies. These will provide an input and alignment into other implementation steps.
- Identify risk architecture.
- Define the roles and responsibilities for conveying prioritization and resource availability.

Step 2: Create a current profile

- Organize an operational level governance group.
- Ascertain availability goals and/or recovery goals for identified systems and assets.
- Review the implementation tiers and record the tier selected by the organization.

Step 3: Conduct a risk assessment AND Step 4: Create a target profile

- Conduct risk assessment to catalog potential risk events to applicable systems and assets.
- For each risk event above, determine potential of that risk being realized and the overall impact on the organization. Think about emerging risks, threat, and vulnerability data.
- Determine the applicability of a subcategory for your organization.
- Determine additional categories of subcategories.
- Complete the Target Profile template, iterating through each subcategory and recording desired state.

Step 5: Determine, Analyze, and Prioritize

- For each subcategory listed in the Target Profile, record the difference between the desired
- capability level and the current state (as described in the current profile).
- Determine required activities for each subcategory to close the gap between current state and
- target state.
- Review the potential activities defined, determine the appropriate priority of those activities. This is to align with risk appetite.
- Determine the resources necessary to accomplish the activities described.
- Create and record an action plan of activities with milestones, ensuring appropriate responsibility
- and accountability, to achieve the desired outcomes according to the determined priorities.

Step 6: Implement action plan

- Consider a continuous feedback loop and metrics development to your governance committee.
- Assist in the resolution of significant issues.
- If necessary, you may need to adjust;
  • The target profile
  • Gap Assessment
  • Action Plan

8.2 Ransomware Risk Management

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) recently issued a Ransomware Profile identifying steps organizations can take to prevent, respond to and recover from ransomware events. According to the profile, its "purpose…is to help organizations identify and prioritize opportunities for improving their security and resilience against ransomware attacks." NIST encourages organizations to use the document as a guide for profiling the state of their own readiness and to identify gaps to achieve their goal.

The profile applies the five foundational pillars of cybersecurity (identify, protect, detect, respond and recover) to ransomware. Based on this framework, organizations should, among other things:

- Inventory assets, systems and processes, including where controls may be shared with third parties;
- Ensure everyone in the organization understands their roles and responsibilities for preventing and responding to ransomware events, with documentation memorializing the structure;
- Establish and communicate policies needed to prevent or mitigate ransomware events, which are in line with legal and regulatory requirements;
- Factor ransomware risks into organizational risk management governance;
- Ensure the ability to receive cyber threat intelligence from information-sharing sources;
- Understand the business impact and expenses of potential ransomware events;
- Implement an incident response plan that appropriately prioritizes ransomware events, has defined roles, contains both technical and business responses and is regularly tested (to ensure the plan and processes match changing organizational needs and structures, as well as new ransomware types and tactics);
- Coordinate ransomware contingency planning with suppliers and third-party providers;
- Conduct ongoing training regarding ransomware threats; and
- Monitor personnel activity to detect insider threats, insecure staff practices and compromised credentials.

NIST's guidance comes on the heels of a variety of measures from the Biden administration to combat ransomware.

Source of information to this article :"McDermott Will & Emery"-
https://www.jdsupra.com/legalnews/nist-issues-cybersecurity-framework-for-3692157/