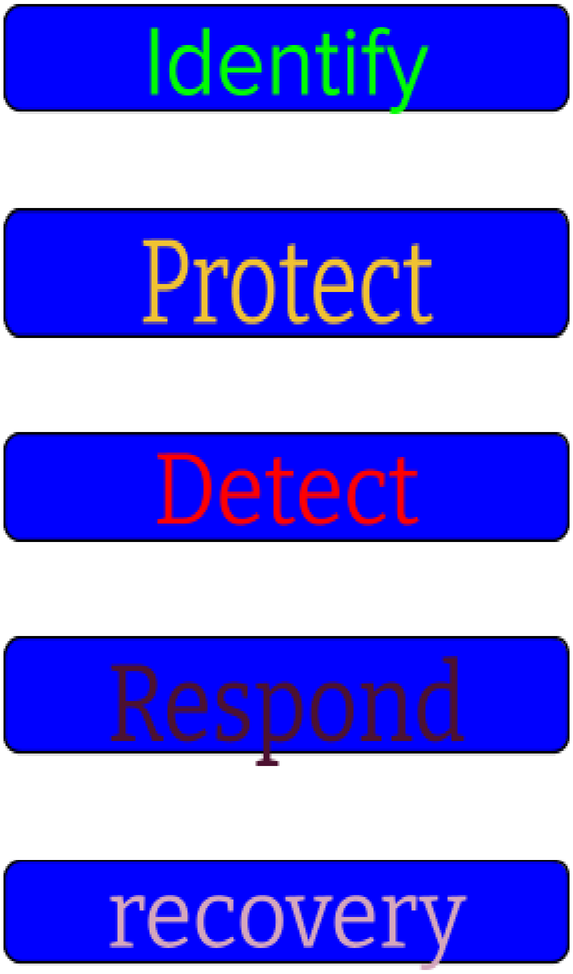
NITS-Cybersecurity Framework



Identify

Protect

Detect

Respond

recovery

This document will cover these five nist cybersecurity framework stages on cybersecurity course college.our goal is to create a strong risk management and useful respond plan based on this framework

For the purpose of a demonstration, we will take a small part of the college's assets and conduct a risk management review on them in a bizarre manner.

Identify

This step is very significant which includes five different parts, and a step in which we have collected all association's assets and created a useful and clear risk management plan.

Five parts that we have to set up very clearly in this stage.

Assets

To make our strategy very effective and useful we have to identify and recognize all association's assets as much as possible.let's set up our different assets.

- Employees and customers - security team, teachers,managers,IT team,students,secretaries, Study Consultant,cyber security department
- Files - customers,employees and students persenality details,study materials
- Servers and computers - web servers,database,ftp server,active directory server,web application firewall,network firewall,switches,routers,printers,security cameras,

Business environment

Domain bussiness

- ★ Cyber security learning course and online cyber security learning course

Assets impact on the business

At this stage we take all our assets into our attention and see clearly the assets' impact on our business in order to be able to create a strong risk management plan.

- ★ Employees and students impact on the business - employees and students may deal with the college’s uniq study materials.for instance the teachers teaching and dealing with different learning stuff like files and another option is that the security team is verifying that strangers can not get into the college without permission etc.
- ★ Files impact on the business - The content and files are what make the college an organization that provides this type of service
- ★ Servers impact on the business - The college has different servers. Some of the servers hold the content that the college offers and some are protecting the organization

Geverence

This section talks about the external regulations on the college and the college standards

- ★ External regulations - Regulation by the banks following the use of students' credit cards, following this regulation it was decided that the college will make a penetration testing on the company's network every year in order to maintain the credit card of its customers and Supervision and control on behalf of government ministries
- ★ The college standards -
  - ➢ Do not put personal computers and disks devices
  - ➢ Prohibition of entry into forbidden rooms
  - ➢ Change passwords every few months

Risk management

- ★ Financial loss - due to damage to the college servers or some cyber security attack or physical theft of one of the prestigious servers of the college,The college may incur a financial loss
- ★ Loss of customers - following to cyber security attack, many students decide to leave college
- ★ Legal trials - Following the theft of students' personal details, students may drown the college
- ★ Loss of reputation of the college - Following some hacking, the college may lose its image

Risk management strategy

★ Buy suitable products - In order to prevent theft or physical vulnerability on the servers the college needs to purchase products That will prevent people from being touched, for example codes at the entrance to server rooms, security cameras etc

★ Buying cyber security products - The college must buy the most advanced products in order to make the most of its Efforts to prevent any hacking its system

★ Allocating a budget for marketing and advertising - If necessary the college may make aggressive publications To attract new customers

Summary: At this stage we examined all the different assets that the college has and what is the impact of each asset on the college, we understood What regulations and standards are there for the organization, we concluded what the potential damage could be to each property and designed a clear plan

Protect

This step talks about protecting the organization itself and its assets. In order to give the best performance at this stage it is very important to know all assets.let's divide this stage into six parts so that we can understand it clearly.

Access control

- Building security guard - The college puts a security guard at the entrance to the building to prevent strangers from entering
- Security Cameras inside the building - The college puts security cameras in order to monitor everything that happens inside the college And outside it
- The college uses advanced technologies to prevent non-professionals from entering into server rooms And into different places
- The college uses advanced technologies to maintain the college's website, database, and servers.for instance firewalls, daf, waf
- To prevent information leaks from staff or students the college uses appropriate technology. For instance nac ,dlp
- The college uses the active directory server to manage its employees and students in an orderly manner

Awareness And Training

- ➢ A lecturer at the college gives a short tutorial to new students on the subject of introducing external components to the college
- ➢ The college requires its employees to have some technological background
- ➢ A college student is required to change a new password every few months
- ➢ Once every few months the founder of the college gives a short tutorial to employees and students on the subject of information security

Data Security

The college uses different advanced tools to protect its files and its valuable contents.all the employees and students personal details are located on the college database system so employees and students may be able to change their personal details.there for the college use vpn service to protect those details.

Info Protect

To protect different dates like user and employees private details ,marketing date from its users and its employees the college is uses advanced tools like web application firewall.

Maintenance

- The college is assisted by a system person in order to keep its system patched and manage file permissions.
- The college has an employee who maintains everything related to the world of users management - firewall's rules,active directory and group police And modifies them as needed and in addition this employee hardens all the rules that are on different servers in order Reduce the attack space on different servers.
- Following regulations applied to the college by the banks, the college annually brings in external professionals in order to check its system protection.

Protective Technology

In this stage we have to tils all out protective technology systems

- Network firewall - creating network access control and monitoring all network traffic
- Dlv - creating some rule to avoiding of stealing from the user and from difference employees departments
- Nac - creating some rules to avoiding of entry an external devices into the system
- Waf - web application firewall to protect the web servers and databases
- Active directory - for management of the users and employees
- Vpn server -to allowing private and secure connection for the users and employees into network

Summary: We have examined at this stage the principles of protection that a college plans to apply and finally we have listed all the technology tools in order to create as effective a protection plan as possible.

Detect

This phase is a phase of identifying and monitoring various threats, this phase uses all the content transmitted to it by all the servers that are under the protection of the organization like log files. Let's divide the phase into three parts so that we can better understand.

Anomalies and events

- The college has a threat detection and monitoring system, this system captures the events and documentation from the various servers and creates for itself Pattern or pattern of network transport behavior, if at any point there is a deviation from the initial pattern of the system, the system need to issue alerts
- **Important emphasis**: When creating the pattern, take into account how clean the initial pattern is from various threats that should not be present within the network, an example of an attack that has occurred in the past.

Security Continuous Monitoring

This is a part where the events in the system are followed for a long time - one of the examples that can illustrate this part is to monitor every entry of students or employees into the system. This type of process gives us control over everyone who connects to our system.

Detection processes

After receiving information from the various processes we have done, we begin to examine each and every event and decide on the significance of the events
Example: If in college we decided to do network monitoring, in this section, we examine the the events we received and decide what each event reveals to us

There are two optionality approaches we may take to look at every events and make decisions.

- **White list** - This approach means creating a list of rules we want to allow and an event that is not in the list is considered an exception.
- **Black list** - This approach is the opposite of the previous approach,in this approach creating forbidden rules and any event that is not on the list is considered a allowed event

Summary: In this section we collected all the events from different servers and created an initial pattern and did monitoring for in-depth analysis and finally defined what our working method is.

Respond

At this stage we are dealing with a response to an incident or cyber issues that have happened, in order to get the best and fastest response It is very important to configure the system identification and monitoring settings in the most professional way

We can divide this section to six parts so we can understand it clearly

Response plan

At this point we are preparing our response plan. A response plan must be built at the stage of a risk management strategy in order to take into account which appropriate components the organization must purchase in order to protect its assets.

Example: One of the risks to the college is the theft of one of the servers. In such a case the response plan is to communicate with the maintenance personnel of the college and use the backup server.

Commencation

This is the stage of managing internal and external communication

Internal communication - communication that is done within the organization for the event, this communication is done between the employees.

For example, similar to the previous phase, at this stage we update the maintenance personnel, the branch managers and everyone who is relevant to the event

external communication - the college decides to publish to the national media about an event that happened.

Analysis

Once we have built a clear response plan this is the part where we examine and test all the intrusions and security vulnerabilities that caused the incident comprehensively

- ➢ the lack of vigilance of the security guard at the entrance is the main cause of theft

- ➢ lack of vigilance on the part of the staff and students led to the arrival of the server room, a malfunction in the alarm system at the entrance to the server room allowed them to enter and take equipment

Mitigation

After an in-depth investigation and diagnosis, at this point our first response is made to get the organization back into full operation

Improvements

Phase analysis and learning about the events that happened.Following the previous example of equipment theft, we understood the sequence of events and at this stage we will make corrections and improvements to the access control of our system.

Example - next time increase the vigilance of security guards,students and staff

Summary: In this section we have defined a clear response plan and through internal or external communication and finally we have implemented improvements

Recovery

Recovery plan

This is a post-event rehabilitation program - in this program we detail our method of rehabilitation in order to return the organization to its previous state. The rehabilitation plan should be clear. For example, if there was a hack in our organization and some of the files were encrypted, in the rehabilitation phase we will take some files from our backup server to restore the organization

Improvement

It is a process of improvement and teaches about the process of rehabilitation - the way we examine ourselves for our method of work during rehabilitation

Cummunicition

- Internal communication: The communication that takes place in the college between the teams in order to carry out rapid rehabilitation,
- External communication: After many efforts by the various staff to return the college to its normal state, the college decides to go to the national communication.

Summary: In this section we have defined a clear plan for returning the college to normal condition after an event and we have learned lessons and improved ourselves