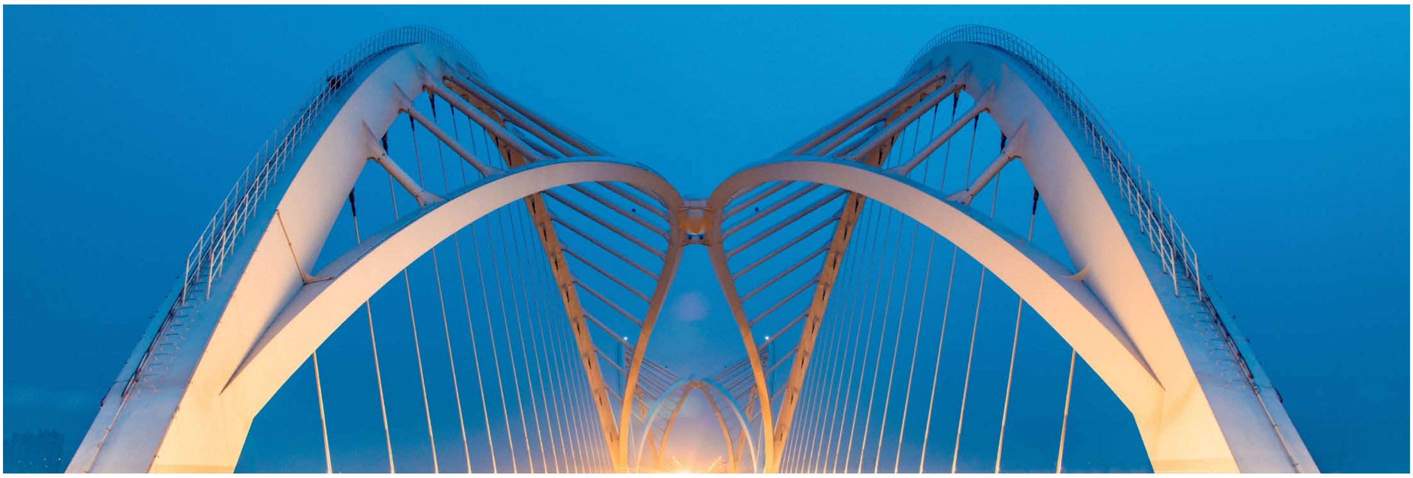
FIFTH STEP WHITE PAPER

# The NIST Framework: Understanding the Protect Function



**The National Institute of Standards and Technology (NIST) Framework provides a common taxonomy and mechanism for organizations to:**

1) **Describe their current cybersecurity posture;**

2) **Describe their target state for cybersecurity;**

3) **Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;**

4) **Assess progress toward the target state;**

5) **Communicate among internal and external stakeholders about cybersecurity risk.**

**The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.**

**In this white paper I will examine the Protect function and what that means for organisations, their IT teams, Chief Risk Officers and the C-suite.**

## Protecting your Data

It is important to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Access control is about protection of systems from a user ID or password or the ability to gain access to systems or data. That can also extend to physical access to infrastructure. You don't want people being able to wander into your servers and gaining physical access, for example.

From a user ID and password perspective there are standard guidelines and best practises around issuing and retiring access to systems and data. They typically mean that people only have access to the data and information and systems that is required for their jobs. The principle of least permissions apply and access should not be shared with a colleague, for example.

## User IDs

So two people who work together should not have the same user ID and password even if we are working in the same role because there could come a time when you leave and I leave and then what happens to that user ID? It still remains mine as opposed to a shared one, what does that mean?

User IDs should be unique to the user and they should go through a life cycle. The life cycle for a user ID is typically created when the person joins an organisation or when they require access to a system. Their user ID is created, and permissions are granted, as that person moves through the organisation it may be that their accesses change. This can take two different forms.

## Access Control

Access to systems can be where you have one user ID that accesses all your systems. That is called single sign on and you are just given permission to access other systems.

Some systems either don't allow interaction with single sign on systems (these are rarer these days, but do still exist) or they are so sensitive that people want to have different IDs and passwords issued.

As you move around the organisation you can gain access to new systems but you also lose access to those systems that you don't require access to any longer. It is about having the ability to switch on or off access as appropriate. You don't want to accidentally breach your segregation of duties by allowing someone to move over to the accounts receivable side of the business and still have access to other parts of the business where it could create a conflict of interest.

The final step of that lifecycle of access management/control is the deletion or retiring of the account. That happens when someone leaves the organisation or when access to that system is no longer needed. User IDs should be reviewed on a regular basis to ensure that access is only available to those require it (and that no-one has been missed from an earlier process).

> "You should start with your new starters, as you mean to go on, and should certainly raise awareness as part of your induction process."

## Cyber Awareness and Training

Part of cyber awareness and training is making sure that there is knowledge within the organisation about cyber threats that it faces. There is no point in doing all the hard work identifying all these issues and risks and potential challenges and then not communicating those within the company because that means the business is not protected to maximum effect.

You should start with your new starters, as you mean to go on, and should certainly raise awareness as part of your induction process. Some organisations store up their inductions over a quarter. A business should not delay cyber awareness for an induction in those cases.

That induction and further awareness and training could be computer based training where employees receive a number of questions where they have to complete a certain pass rate, typically 70% in the insurance world, for example. These computer-based exercise can be quite simplistic, however, a little dry or not as engaging as having someone talk you through the challenges with respect to cyber security and the scenarios the company is trying to protect against or has identified in the identify phase.

> "I recall an example where there was an attachment of a naked celebrity and people were calling the IT service desk because this attachment wasn't opening."

## Beware the Naked Celebrity

Insurance organisations don't take cyber training and awareness-raising nearly seriously enough. I recall an example where there was an attachment of a naked celebrity and people were calling the IT service desk because this attachment wasn't opening. They couldn't see a photo! What was actually in that mail was not a photo, it was actually a virus.

The machines were very quickly infected and part of that virus was mailed to other people with the same message which spread throughout the company fast. Action had to be taken promptly in order not to overrun the company's servers, with potentially millions of emails being sent internally and externally from within the company with this virus. Naked celebrities clearly have a lot to answer for!

Associate companies and service providers should be included in your awareness process. You want to make sure that they understand the base level of understanding that you expect them to have. The form that this awareness takes will vary according to your organisation, but should include a face to face element with your account representatives.

## An Open Culture

Organisations that deal with the evolving security risks, are those that encourage a culture where people are not embarrassed to put their hand up when they think they have seen something suspicious or unusual.

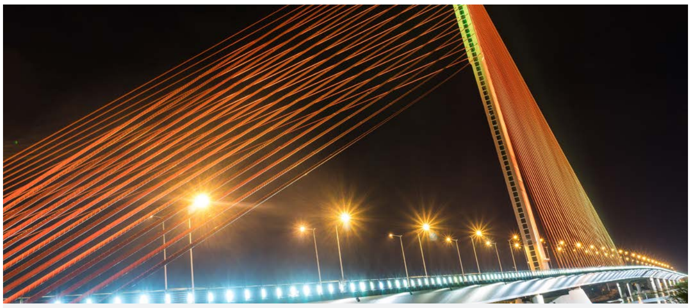
People's instincts are hardwired and they should use them. For example, if an employee has noticed that there a number of files in this directory, which contain a number of credit card details and numbers. Raise it as an issue. Something like: "This may be a bit of a silly question but I don't think these details should be there."

People should feel able to report incidents quickly without fear of being labelled as alarmist even if it turns out to be a false alarm. In the U.S. on the subway system they say "if you see something say something" which is a nice turn of phrase. Raise awareness.

### Cyber Protection and Data Security, Processes and Procedures

Know what the criticality and sensitivity of your data is. Assess your data's criticality to the business. Understand what your data assets are.

Having identified these, you need to understand their level of criticality. Make sure you have user access control in place. Are you encrypting all the data in your databases, is it appropriate for you to do so, will it provide protection if you do? What is the level of encryption and what about data at rest?



> "What standards have you set around data encryption?"

What standards have you set around data encryption? Is it all data for example or is it only personal identifiable information that is encrypted? Or is no data encrypted? There may be a perfectly acceptable business reason for that but it needs to be highlighted and sense checked.

I have covered elements of Information Protection Processes and Procedures in previous articles I have written but essentially it means organisations committing to placing cyber security at the heart of their organisation. This commitment should extend across the business. Certainly within the IT department as a minimum there needs to be standard processes and procedures that have security at their heart.

### Patch Management

Patch management should be in place for all organisations, ensuring that servers are updated to the appropriate levels of software, and security patches released by operating system and software makes applied. Microsoft, for example, have patch Tuesday.

Make sure that you have processes and procedures in place to implement updates and patches safely. Do not just take it for granted that Microsoft have done their job, or that your software or configuration is slightly different. So applying the patches or updates in a test environment before being applied to your live servers is the correct and best practise approach.

> "Not applying patches promptly can mean that your organisation may be at risk of hackers utilising flaws that have already been fixed."

Not applying patches promptly can mean that your organisation may be at risk of hackers utilising flaws that have already been fixed. The release of a security patch can act as a press release to hackers, who can look at the software released and understand the nature of vulnerability, they can then target un-patched computers, or perhaps just create a "virus" that gets spread, but will only be able to attack un-patched computers.

An often underplayed part of protection is an organisation's polices. Have the appropriate policies in place and ensure that there is a good understanding of what these are. Ensuring that policies are reviewed regularly to ensure that they have the right level of information and cyber security protection for your organisation as it exists today, can make the difference between your organisation being the victim of an attack, or having a near miss.

### Protective Technology

This is my last blog in the recent series I have been writing about Protect part of the NIST cybersecurity framework. So far in In this series I have covered Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures. This concluding blog focuses on Protective Technology.

There are a number of different types of protective technology software but the key ones are obviously having firewalls, which can take different forms. Most organisations have firewalls that are hardware firewalls, but most modern computers have a software firewall this works in a similar (although not as sophisticated) was as a hardware firewall, which means that only the internet traffic that you want to allow in is permitted to come through the "door".

> “A computer without a firewall is a bit like having all the doors and windows in the building open and unguarded...”

## Preventing Unfettered Access

A computer without a firewall is a bit like having all the doors and windows in the building open and unguarded, offering unfettered access. Anyone can climb in through the windows and rummage around. A firewall locks down all doors and windows, and puts a bouncer on the front door.

Malware protection or antivirus software as it is known to the general public provides protection from malware, which is software that is written to do something that the user is not expecting. Antivirus software is not infallible though, and it too must be kept updated. Antivirus software usually uses a virus definition file to recognise malware, this file is usually downloaded from a corporate server or from the antivirus manufacturer’s servers. Without the latest virus definition file, the software won’t be able to recognise a virus, so it’s vital that it is kept up to date.

The last type of protective software that I’ll cover in this article is intrusion detection software. This can take various different forms, but all of them have the same function of allowing enterprises to monitor Internet and internal network traffics for activity that is unusual, or suggests that the organisation is being attacked by a hacker or that a machine on the network has been infected by malware.

## Luring the Hacker into the Cyber Honeypot

A honeypot is computer system that appears to contain something of interest to a hacker, or that appears to be unprotected, thus attracting the attention from those targeting the organisation.

In reality honey pots are not what they seem to be, they are in fact sophisticated tools that allow IT teams to identify potential issues and then take appropriate action. This is similar to the police baiting a criminal and then conducting undercover surveillance, and finally punishing the criminal.

This concludes this white paper on the Protect function, which forms part of the NIST cyber framework.

To summarise, it is important to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome categories within this function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

> “In reality honey pots are not what they seem to be, they are in fact sophisticated tools that allow IT teams to identify potential issues and then take appropriate action.”