**Chapter 6**

**Handling Cyber Assets**

A **cyber asset** is a programmable electronic device (computer cell phone or any such device) and communication networks including hardware, software and data.

Cyber asset does not include removable media like storage media or external hard drives. A cyber asset is also called a cyber space asset. These assets are essential for reliable operation of a critical asset. The cyber asset participates in supervision or

autonomous control which is essential for reliable operation of the critical assets like

servers, defence control systems etc.

 Handling cyber assets means implementing successful cyber security or

providing successful solution for cyber asset protection subscription. The NCCE

(National Cyber Security Center of excellence) at NIST (National Institute of

Standards and Technology) provides most pressing cyber security problems with

practical and standard based solutions using commercially available technologies. It

collaborates with Academics, Industries and Government experts to build modular,

open, end to end reference designs that are applicable. NIST cyber security practice

guides specify cyber security challenges in the public and private sectors. These

guides are more user friendly and with practical approach. They are facilitated with

standard based cyber security approaches. They contain example implementations of cyber security practices but they do not describe regulations and they do not carry

statutory authority.

**6.1** **WHAT IS CYBER SECURITY**

Cyber security means protecting your computer, network, data and information

from major cyber threats and attacks. It is the state of being protected from the

unauthorized use of electronic data as well as damage to cyber assets. It is a critical

issue for all businesses and defence systems. It includes security or protection from

theft, damage and loss of hardware and software both. For any organization having

cyber assets, cyber security is an important challenge. Every such organization

needs to build a proper configuration policy for managing cyber assets. The cyber asset configuration management policy includes the purpose of securing both

hardware and software assets along with information.

**6.2 CONFIGURATION MANAGEMENT**

The configuration management technologies help the security administrators to

view and change the security settings on the network and hosts, verify the

correctness of security settings and maintain the operations in a secured manner.

Such technologies include policy enforcement tools, continuity of operations tools,

scanners for testing and auditing security and patch management. The configuration

management tools define a set of security rules called configuration policy, with a set

of security configurations like pass word managers, pin code managers, system and

file access managers etc. The most important part of configuration management is

configuration management policy.

**6.2.1 Configuration Policy**

A configuration policy provides tools to help administrators define and ensure

compliance with configuration and security rules. A configuration policy can be

designed after identifying risks and threats. After that policy definition is

established with baseline policy settings. Policies can include the features like user

rights, group rights, minimum password requirement etc for specific applications.

After defining the policy various tools can be used for compliance checking. For

example testing for a particular configuration on a subset of computers or checking

that console passwords fit the policies of organization etc. Then comes the phase of

reporting which includes reports for configuration along with description of user

accounts, access controls, and other software patch levels. Some polices include

remedial tools also that allow to install latest security software patches.

 Thus, a **configuration policy** may be defined as a set of access controls and

configurations that affect the overall security of a user, group, device, application or

cyber assets of a system or organization. All organizations should have properly

documented configuration policy with purpose, scope, roles, responsibilities,

management commitment, coordination among organizational entities and

compliance.

 There can be two types of configuration polices in an organization

* Information configuration policy
* System configuration policy

The Information configuration policy enforces the security of data, software and

information flow of the organization. System configuration policy, on the other hand

ensures the security and consistency of company devices or hardware supports. Such policies are applied to all information systems. They compose boundaries of the organization and provide efficient ways to upgrade system equipment. They avoid conflict problems and save system memory and companies both.

 The configuration policy in fact includes all about configuring the system or

organization for secured working. Along with all its working it also includes overall

requirements of hardware and software tools for security. Generally creating a

configuration policy needs settings of IO devices, work devices, OS, terms and

conditions etc. After creating a policy it is deployed.

 Management of policy includes edition, deletion and deployment of the policy.

Whenever a configuration policy is enforced it also needs a policy for disposal of the

assets. It is called disposable policy.

**6.2.2 Disposable Policy**

A policy that defines rules, terms and conditions for disposal of cyber assets

which are either damaged or harmful for the organisation. With time some things in

configuration policy become obsolete. At that time there comes a need of upgradation and removal of obsolete items both. This removal of obsolete hardware and software asset is done as per a policy which is defined during the development stage of the security policies. The configuration policy is used to configure the system. Then management policy manages as per the conditions, circumstances and requirements. It also allows editing, deploying and deletion of configuration policy. At the same time the disposable policy explains terms and conditions along with rule regulations of removal or disposition.