**Cyber Security of**

**DoO(C&S)**

By Sreejit Das

**CYBER SECURITY OF DoO(C&S):**

**Abbreviation table**

|  |  |
| --- | --- |
| **POST NAME** | **FULL FORM** |
| **CIRA** | **Centre for Intelligence Research and Analyses** |
| **CERT-IN** | **Indian Computer Emergency Response Team** |
| **CCMG** | **Cyber Crisis Management Group** |
| **CCMP** | **Cyber Crisis Management Plan** |
| **CISO** | **Chief Information security officer** |
| **CSG-DDP** | **Cyber security group - DDP** |
| **DDP** | **Department of Defense Production, Ministry of Defense** |
| **NDA** | **Non disclosure agreement** |
| **IT** | **Information Technology** |
| **IT/OFBHQ** | **IT section of OFB Headquarter** |
| **LCSC** | **Local Cyber Security Cell** |
| **LCSO** | **Local Cyber Security Officer** |
| **SCSC** | **Sectoral Cyber Security Cell** |
| **SCSO** | **Sectoral Cyber Security Officer** |
| **ISO** | **International Organization for Standardization** |

**Cyber Security**

**Aim:** The main objective of cyber security is to protect organizations from cyber threats and ensure the CIA (**Confidentiality,Integrity,Availability**)

* **Confidentiality**

Confidentiality is the protection of information in the system so that an unauthorized person cannot access it. This type of protection is most important in military and government organizations that need to keep plans and capabilities secret from enemies.

* **Integrity:**

Integrity is the protection of system data from intentional or accidental unauthorized changes. The challenges of the security program are to ensure that data is maintained in the state that is expected by the users.

* **Availability:**

Availability is the assertion that a computer system is available or accessible by an authorized user whenever it is needed.

**How does it work:**

* **Governance:**

cyber security governance is the process of establishing the architecture that ensures a company's security programs align with business objectives, comply with regulations and standards, and achieve objectives for managing security and risk.

* **Technology: operations:**

Technology is vital for cyber security, offering tools to safeguard information and networks. Firewalls, encryption, and biometric authentication are key examples. AI and machine learning improve threat detection, while blockchain ensures data integrity. As the cyber landscape evolves, innovative technologies are crucial in the ongoing fight against threats.

The latest technologies in cyber security include :

* Artificial Intelligence (AI) and Machine Learning (ML)
* Block chain
* Cloud Security
* IoT Security
* **Operation**

In cyber security, operations involve protecting systems, networks, and data from threats through tasks like monitoring, analyzing logs, implementing controls, and responding to incidents.

**SCOPE:**

The scope of cyber security is wide, covering network security, application security, data protection, incident response, risk management, and compliance. It also includes emerging technologies and the protection of sensitive information.

There are various steps which can be taken by the organizations to save the data

* Protecting and recovering networks, devices and programs from any kind of cyber attacks
* Saving personal data as well as business data
* Planning, designing, and implementing security measures and controls
* cryptographic controls

**Cyber Security Policy:**

A cyber security policy is a set of guidelines that outlines how an organization protects its information systems and data from cyber threats. It defines roles, security controls, incident response, and employee training.

**Some Terminology used in Cyber Security:**

Asset:

In cyber security, assets are valuable resources that organizations protect. These include data, systems, applications, networks, intellectual property, and physical devices.

Threats:

In cyber security, threats refer to potential risks or dangers that can exploit vulnerabilities in systems, networks, or data, resulting in harm or damage.

Risk:

Risks in cyber security are potential negative consequences from vulnerabilities being exploited. They include data breaches, service disruptions, financial loss, reputational damage, and regulatory non-compliance.

Controls:

Controls in cyber security are measures to mitigate risks and protect against threats. They include preventive, detective, and corrective controls. Administrative controls establish policies and procedures, while technical controls use technology like encryption and authentication.

**Cyber Security Policies of DoO(C&S):**

Cyber Security of DoO(C&S) is maintained by

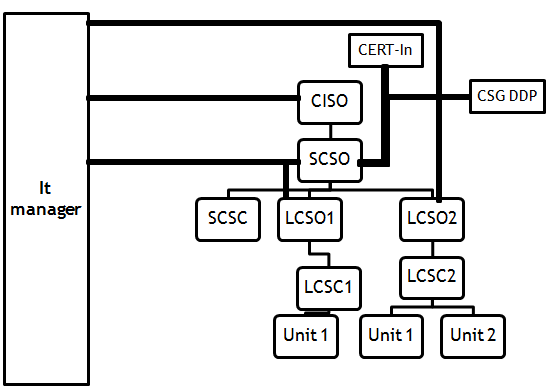
* **Cyber Security Policy 4:** It maintains ISO27001and ISO27002
  + **ISO 27001:** Defines the requirement of an ISMS
  + **ISO 27002:** It tells more about physical element security
* **Cyber Crisis Management Plan 4.0**
* **CSF-DDP:** It is a framework structure maintained followed and responded by Security system. Created by CSGDDP
  + Mainly works as target fixing and achieving guideline.

**ISMS:** ISMS stands for Information Security Management System. It is a systematic approach to managing sensitive information and protecting it from unauthorized access, disclosure, alteration, or destruction.

**Cyber Security Policy 4**

|  |  |
| --- | --- |
| * **Direction by**    + DDP(Department of   + Defense Production) * **Revised by**   + SCSC * **Aligned with**    + ISO 27001   + ISO 27002. | * **Approved by:**   + Member   + CISO   + Chairman |

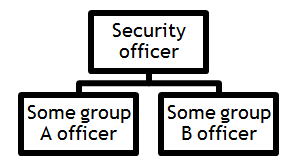
**Hierarchical structure :**

****

|  |  |  |
| --- | --- | --- |
| **POST/Sec Name**  **/Organization** | **DESCRIPTION** | **WORK** |
| **LCSC** | Cyber security cell for every unit | 1)Reply to the advisories from SCSC  2)Implementation of best IT practices  3)Intra factory Audit conduction |
| **LCSO** | Head of LCSC | 1)Reporting officer of LCSC  2)Head auditor of Intra Unit audit |
| **SCSC** | Central Cyber Security cell | 1)Organisation wise Cyber security program  2)Directives to conduct AUDIT  3)Training of Technical employs  4) Following CSG DDP given IT security protocol. |
| **SCSO** | Head of SCSC | 1)Reporting officer of SCSC  2)Cyber Crisis Management response |
| **CISO** | A Member nominated by  Chairman  Head of Cyber Security | 1)Brief the Progress in every 4 months  2)Commanding officer of SCSC LCSC & IT  3)Audit monitoring  4)Review observation  5)Disaster Recovery |
| **IT managers** | Managers working at IT | 1)Report CISO, SCSO, LCSO  2)Do risk assessment  3)Prepare plans  4)Cyber Security awareness |
| **CSG DDP** | Central Cyber security group | 1)Passing different policies  2)Reporting Incidents |
| **CERT-In** | Central Cyber Emergency Response Team | 1. It is the national agency responsible for dealing with cyber security incidents in India. 2. Its primary role is to provide timely warnings, detection, and response to cyber security incidents and coordinate with various stakeholders. |

**Some points mentioned in the policy:**

* **Safety of assets** (control mentioned in ISO27001 A.8)
* Record of assets should be kept with all details like owner details and the details of asset
* Asset owner are responsible for safe custody of asset
* **Safety of mobile devices** (control mentioned in ISO27001 A.6.2)
* Mobile Devices should not be lost or compromised.
* Mobile Devices Should not be connected with any external source except intranet or internet of organization.
* A Sop must be there covering damage, theft protection and unauthorized access.
* **Safety of Human resources** (control mentioned in ISO27001 A.7)
* The organization
* Spread Awareness among new human resource
* educate and train them.
* Introduce them to policy updates
* The only necessary documents for work are provided to new human resources.
* Every working personnel should Get it/ict /ot resource in ethical manner
* All violations in rules are tracked in
* Negligence by any personnel is not allowed
* **Media management** (control mentioned in ISO27001 A.8.3)
* The media is made unrecoverable and removed when it is no longer required.
* The record has been kept of the removed media.
* Cryptographic method is used on media to keep it safe if needed.
* The data is transferred to new media before the removal of that media
* Important data is stored in different media
* Identification of media is required for secure disposal.
* Damaged media device are preferred to be destroyed rather than to be taken to repair.
* Encryption is used to stop unauthorized access
* **Access control** (control mentioned in ISO27001 A.9)
* Access control plan, made by IT contains
  + - Data of User and their privileges.
    - Only the necessary network access is given to the user
    - Different accesses & privileges can be given to the users & also can be taken up
    - User access rights are reviewed in a regular interval.
    - All source code are secured by password
* **Communication safety** (control mentioned in ISO27001 A.13)
* All the systems are connected to the scanner and printer by the a common network and that network is secured.
* Only authenticated systems allowed to connect with the network
* Cd writers and USB ports are monitored/removed
* **System development and maintenance** (control mentioned in ISO27001)
* Any formal changes goes through IT section before making it Final.
* Record is kept of the changes made
* In case of changes to OS of Servers no OS facilities should be compromised
* If outsourcing is done It should be monitored thoroughly
* **Audit**
* Audit is a process in which it is checked that if the system is working maintaining the security and security policy norms or not in every certain period of time.
* Audit is done in three ways Intra Unit, Inter Unit, External.
* **Physical equipment safety** (control mentioned in ISO27001 A.15)
* One Security officer is kept in responsibilities of physical equipment



* A Secure area plan is made by IT section,&Security officers approved by CISO
* The Security strength of perimeter is measured (ex:CCTV, electric fence)
* The organization security makes sure that only the authorized person gets entry & no-one else
* The organization security makes sure that visitors are authenticated.
* Keep a track of medias which are assigned to the employees
* Keeping detailed log for Audits
* Protection is taken against environmental and external threats

**Security Elements:**

* **Organization Network Security:**

**Internet:** The internet is a global network connecting computers and devices, allowing communication, information sharing, and access to services worldwide.

**Intranet:** Intranet is a private network for internal communication, collaboration, and information sharing within an organization. Confidential data is kept here.

* Air gap maintained between Internet and Intranet
* **Antivirus:**

Antivirus software detects and eliminates malware, protecting devices from online threats. Regular updates are essential to maintain its effectiveness against emerging risks, making it a critical component for safeguarding system security.

* Anti virus is Installed in System
* It gets updated daily patch
* It logs malicious virus and negates it
* Only White listed USBs are allowed in any computer
* **Firewall:**

A firewall is a network security device that filters and monitors network traffic, protecting against unauthorized access and malicious activities, serving as a crucial defense mechanism for network security.

* Blocks certain websites and gives report to the authorized person through its policies when anyone tries to access them.
* The authorized personal can edit/change the list of blocked/locked websites.
* If there is any malicious virus in the computer firewall takes care that the whole network doesn't get infected.
* **Centrally controlled all client computers(Domain Controller):**

A domain controller is a server that manages security, authentication, and access control within a Windows domain, allowing centralized management of users, computers, and resources.

* 435 Intranet computers and 160 Internet computers all are observed by the administrator.
* The administrator can observe invalid requests; if necessary allow some request or block them.
* It is used to grant different requests to different users.

**Audit:**

Audit is a process in which it is checked that if the system is working maintaining the security and security policy norms or not in every certain period of time.

* Audit is done in three ways Intra Unit, Inter Unit, External.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Auditor** | **Co-opt** | **Frequency** |
| Intra Unit Audit | LCSO | Officers of JWM level | 1/year |
| Inter Unit Audit | * Nominated by SCSC * Not in audit unit | -- | 1/year |
| External Audit | * CERT-in given auditor * From any PSU or Government office | --- | 1/year |

**Some points of Audit:**

* External Auditor must sign NDA promising making things confidential.
* The auditor reports to the head of audit unit and CISO.
* Audit logs are restricted to CISO, SCSO, LCSO .
* To minimize disruption of the regular work flow audit is done only on ROM
* Work
  + Audit team Checks all cyber security measures are taken or not
  + If any problem is there audit team and auditor decide what action has to be taken.
  + Audit team and auditor give recommendation for improvement.

**CYBER CRISIS MANAGEMENT PLAN(CCMP):**

**Released by:**

* CERT In
* Meity
* Government of India

**Signed by:**

* JWM/IT
* JWM/e-Admin
* Assistant Director/IT
* Deputy Director/IT
* Director/BSG
* DDG/IT
* CISO

**Cyber Events, Incidents, Crisis:**

**Event:**

* Any observable occurrence in a system or a network is called a cyber Event

**Incidents:**

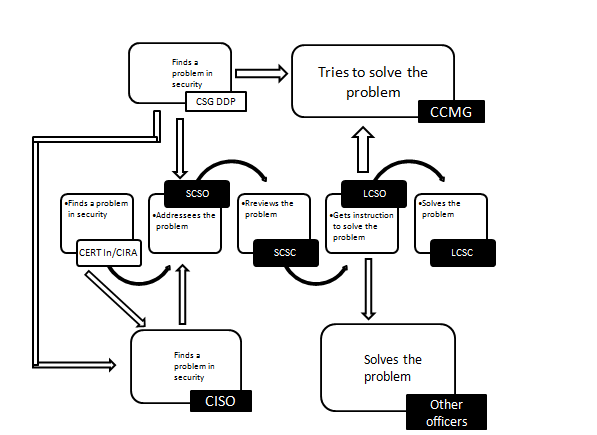
* A cyber incident is a cyber event.
* A cyber incident causes, or may cause a breach of information security in respect of availability, integrity & confidentiality.

**Crisis:**

* In a cyber crisis breach of information happens.
* In a cyber crisis breach of security communication with CSG-DDP happens
* Organization Internet based applications are compromised in a cyber crisis

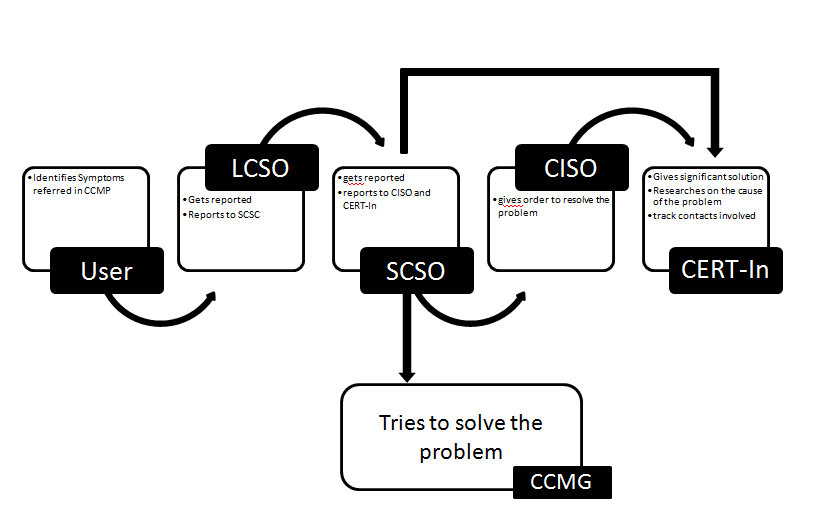
**When a high authority finds security problem:**

1. CERT In or CIRA reports CISO or SCSO with the problem (and sometimes the direction to solve it)
2. If CSG-DDP finds any problem they reports CISO or SCSO and they also inform CCMG
3. CISO reports SCSO
4. SCSO informs SCSC about this
5. LCSO of the unit( in which the problem has been found) is reported
6. LCSO tries to resolve the problem following the directions given with the help of LCSC , CCMG and a group of chosen officers



**When a user finds a security problem:**

1. User finds a problem and report to the LCSC & LCSO of the unit
2. LCSO reports the SCSO if it is really a security problem
3. SCSO reports CISO and also inform CCMG(sometimes CERT-In also) about the problem
4. CISO reports CERT-In for remedy and further research
5. LCSC & LCSO receives directives from CCMG/ CERT-In and then they implement it to solve the problem

****

**Connection with external government organizations**

* **CERT-In:** A Computer Emergency Response Team (CERT) is a group of information security experts responsible for the protection against, detection of and response to an organization's cyber security incidents in India.
  + They inform us when cyber problem appears
  + We report them about any cyber problem.
* **CIRA:** The Centre for Intelligence Research and Analyses (CIRA) seeks to promote thought leadership and research in the field of intelligence studies.
  + Informs us about threat.
  + Gives us advisory about tech.
  + We reply them
* **CSG DDP:** Cyber Security Group Of Department of Defence Production
  + They inform us instruction to go by
  + They conduct the ministerial audit.
  + We contact them in cyber crisis
  + They inform us about any cyber incident they find out.
* **MEITY:** Ministry of Electronics and Information technology
  + They helped issuing CCMP4.0
  + ISO: International Organization for Standardization
  + We maintain ISO27001 and ISO27002.

\*\*\*\*\*\*