1. What is security
2. What is E-security
3. Shift of department from Manual to system
4. Why CBEC needs E-security
5. Tools used in E-security
6. Progress till date
7. Challenges faced with current examples
8. Solutions & suggestions

Security

It means protection of a person, building, organization, or country etc against threats such as crime or attacks by domestic/local/foreign countries etc.

E-Security

- In information technology, security is the **protection of information assets** through the use of technology, processes, and training.
- It include tenets of computer, internet, data, application, information, network & endpoint security in IT realm

CBEC: From Manual to Digital Era

Excise & Service Tax:

Earlier : Return, duty payment & registration were all manual

Present: It is replaced by ACES, e-payment & online registration

Customs:

Earlier: Filing, assessment, duty payment manual

Present: Filing of B.E/S.B, IGM/EGM etc - ICEGATE

Assessment - EDI system

Duty Payment - Online payment

Online Services of CBEC

http://www.cbec.gov.in/htdocs-cbec/online-services

Online Services of CBEC

1. SMS Query
2. Help Mail
3. e-filing of Customs Documents
4. e-filing of Central Excise and Service Tax Returns
5. e-payment of Central Excise and Service Tax
6. Software for Remote Filing (RES PAckage) free download
7. Document Tracking at ICEGATE
8. IE CODE/BIN status
9. Online filing through ICEGATE

Why Need E-Security

Secrecy/Confidentiality

- Protection against unauthorized data (Govt & stakeholders) disclosure
- Technical issues

Privacy

- The ability to ensure the use of information about oneself
- Legal Issues (Article 21)

Integrity

Preventing unauthorized data modification by an unauthorized party

Necessity

Preventing data delays or denials (removal)

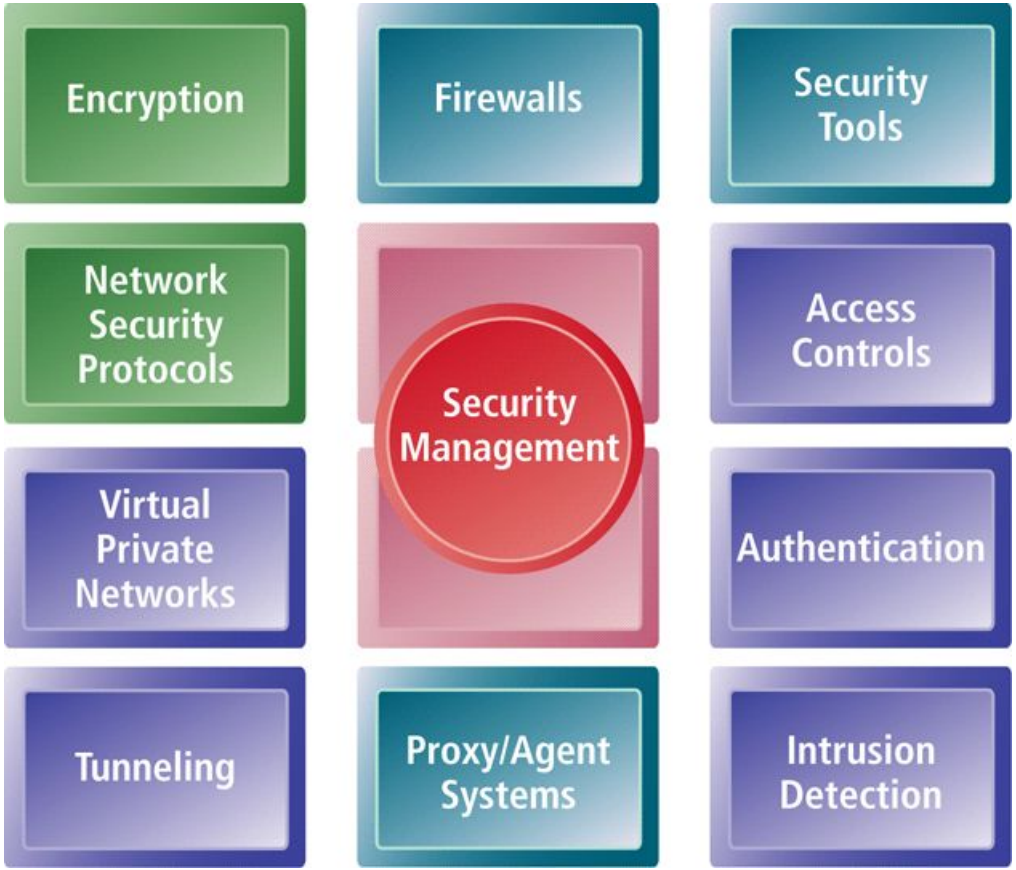
Nonrepudiation

Ensure that e-commerce (online payment at CBEC gateways) participants do not deny (i.e., repudiate) their online actions

Authenticity

The ability to identify the identity of a person or entity with whom you are dealing on the Internet/network

Tools for E-Security



Encryption

1) Transforms plain text or data into cipher text that cannot be read by anyone outside of the sender and the receiver.
   Purpose:
   a) to secure stored information
   b) to secure information transmission.

2) Cipher text
   a) text that has been encrypted and thus cannot be read by anyone besides the sender and the receiver

3) Symmetric Key Encryption
   a) DES standard most widely used

Tunneling

Tunneling is a protocol that allows for the secure movement of data from one network to another. Tunneling involves allowing private network communications to be sent across a public network, such as the Internet, through a process called encapsulation. The encapsulation process allows for data packets to appear as though they are of a public nature to a public network when they are actually private data packets, allowing them to pass through unnoticed.

Tunneling is also known as port forwarding.

Firewall

1) Software or hardware and software combination installed on a network to control packet traffic

2) Provides a defense between the network to be protected and the Internet, or other network that could pose a threat

3) Characteristics

   a) All traffic from inside to outside and from outside to inside the network must pass through the firewall
   b) Only authorized traffic is allowed to pass
   c) Firewall itself is immune to penetration

4) Trusted networks are inside the firewall

5) Untrusted networks are outside the firewall

6) Packet-filter firewalls
   a) Examine data flowing back and forth between a trusted network and the Internet

7) Gateway servers
   a) Firewalls that filter traffic based on the application requested

8) Proxy server firewalls
   a) Firewalls that communicate with the Internet on the private network's behalf

Network security protocols

Network security protocols are primarily designed to prevent any unauthorized user, application, service or device from accessing network data. This applies to virtually all data types regardless of the network medium used.

Network security protocols generally implement cryptography and encryption techniques to secure the data so that it can only be decrypted with a special algorithm, logical key, mathematical formula and/or a combination of all of them. Some of the popular network security protocols include Secure File Transfer Protocol (SFTP), Secure Hypertext Transfer Protocol (HTTPS) and Secure Socket Layer (SSL).

Proxy Agent

A proxy agent is a network management element which acts as a middleman between a management system and an unmanaged device, allowing management by proxy. The proxy agent appears to the device or client as the server itself so it is also an element of security since the management server is completely invisible to connected devices. There are many types of proxy agents meant for different purposes, such as SNMP proxy agents, WINS proxy agents and DHCP proxy agents.

Current Progress

Public Private Partnership (PPP)

CBEC has partnered with TCS, Infosys, Oracle, WIPRO & NIC for securing its critical digital infrastructure & deployment of its digital services.

Regular training of officers and New Recruits

Capacity building in security skills through training & awareness sessions at different dedicated institutes like CFSL, Gandhinagar; SVPNPA, Hyderabad; CEIB Delhi etc

USE of Digital Signatures in Customs

- Authenticates the identity of the sender of a message, or the signer of a document,
- can be automatically time-stamped
- Cannot be imitated by someone else
- sender cannot easily repudiate it later

Challenges of Today in E-Security (GST & Customs)

Tension Between Security and Other Values (Philosophical Challenge)

Ease of use

Often security slows down processors and adds significantly to data storage demands. Too much security can harm ease whereas not enough can mean going out of business.

Public Safety & Criminal Use

Claims of individuals to act anonymously vs. needs of public officials to maintain public safety in light of criminals or terrorists.

Cyber-Espionage - Hackers exfilterate the intellectual property data submitted by stakeholders of CBEC e.g Hackers can intrude into the ICEGATE system to filter out importers & exporters proprietary data

Cyber-crime - Attack of Virus, macro virus, trojan horse, zombie etc. Monthly more than a million attack occur on CBEC system. A recent breach at ICD Tughlakabad, Delhi where hackers have increased the value of FPS scripts .

Cyber-vandalism - Defacing web pages or use DDOS to take them down. Recently NACEN website was defaced by Pakistani hackers.

Cyber-Sabotage - This has the most serious implications and includes DDOS, destruction of data, insertion of malware and logic bombs

Cyber Espionage

Organisation are also reluctant to disclose any attacks and exfiltration of data, both because they could be held liable by their clients and also because they may suffer a resultant loss of confidence of the pub

DDoS Attack

In computing, a **denial-of-service attack** (**DoS attack**) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.[1] A DoS attack is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations.

- ★ Basic tools - antivirus, firewall, better encryption
- ★ Better Software - Bug Free apps, before releasing into systems there should be standardisation and testing of software products to reduce the opportunity for hackers just like apple mobile apps
- ★ Critical Infrastructure - Reducing supply chain risks, Creating a secured Ecosystem
- ★ E-Security Training - Cyber security education, R&D and capacity building of officers in cyber forensics
- ★ Authenticator App - for every officer for logging into system - prevent shoulder snooping, unauthorized access
- ★ Website Shielding - Using Web Application Firewall (WAF) to protect against cross site scripting (XSS), SQL Injection, DDoS attack. It protect servers mainly.
- ★ E-Security Audit - Security penetration testing by professional auditors periodically. Target should be to achieve ISO/IEC 27001:2013 standards.

Thank you for listening!

Any Questions

Digital Signatures in CBEC

- An electronic and Digital Signatures
  - Authenticates the identity of the sender of a message, or the signer of a document,
  - Or ensures that the contents of a message are intact.
- Digital Signatures features:
  - Are easily transportable,
  - Cannot be imitated by someone else,
  - And can be automatically time-stamped.
- The ability to ensure that the original signed message arrived means that
  - the sender cannot easily repudiate it later.