Subject Name: Cyber security

Faculty Name: Dr.A.Vijendar

Module I

Definition of security:

No organization can be considered "secure" for any time beyond the last verification of adherence to its security policy.

Security Features:

Confidentiality: it is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. The Assurance that information is shared only among authorized persons or organizations.

Integrity:

The Assurance that the information is authentic and complete. Integrity In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

Availability:

Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them. Availability of information refers to ensuring that authorized parties are able to access the information when needed.

Concept of Cyberspace

Cyberspace is "the environment in which communication over computer networks occurs. “, and almost everybody in one way or the other is connected to it.

Concept of Cybercrime

Computer crime, or cybercrime, is any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target

Concept of Cyber security

Def: Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

----University of Maryland University College

The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this. 'Some people have argued that the threat to cyber security has been somewhat inflated'

Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

The general security objectives comprise the following: Availability, Integrity, which may include authenticity and non-repudiation o Confidentiality.

Defining a cyber security policy:

Cyber security procedures explain the rules for how employees, consultants, partners, board members, and other end-users access online applications and internet resources, send data over networks, and otherwise practice responsible security. Typically, the first part of a cyber security policy describes the general security expectations, roles, and responsibilities in the organization.

Stakeholders include outside consultants, IT staff, financial staff, etc. This is the "roles and responsibilities" or "information responsibility and accountability" section of the policy.

The policy may then include sections for various areas of cyber security, such as requirements for antivirus software or the use of cloud applications. The SANS Institute provides examples of many types of cyber security policies. These SANS templates include a remote access policy, a wireless communication policy, password protection policy, email policy, and digital signature policy.

Organizations in regulated industries can consult online resources that address specific legal requirements, such as the HIPAA Journal's HIPAA Compliance Checklist or IT Governance's article on drafting a GDPR-compliant policy.

For large organizations or those in regulated industries, a cybersecurity policy is often dozens of pages long. For small organizations, however, a security policy might be only a few pages and cover basic safety practices. Such practices might include:

- Rules for using email encryption
- Steps for accessing work applications remotely
- Guidelines for creating and safeguarding passwords
- Rules on use of social media

Cyber security regulation

It comprises directives that safeguard information technology and computer systems with the purpose of forcing companies and organizations to protect their systems and information from cyber attacks like viruses, worms, Trojan horses, phishing, denial of service (DOS) attacks, unauthorized access (stealing intellectual property or confidential information) and control system attacks. There are numerous measures available to prevent cyber attacks.

There have been attempts to improve cyber security through regulation and collaborative efforts between the government and the private sector to encourage voluntary improvements

to cyber security. Industry regulators, including banking regulators, have taken notice of the risk from cyber security and have either begun or planned to begin to include cyber security as an aspect of regulatory examinations.

Module II

Objectives of Cyber Security

1) To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

2) To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).

3) To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

4) To enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.

5) To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24×7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.

6) To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition, diffusion and commercialization leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.

7) To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.

8) Create workforce of 500,000 professionals skilled in cyber security India in 5years through capacity building, skill development and training.

9) To provide fiscal benefits to businesses for adoption of standard security practices and processes.

10) To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft.

11) To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.

12) To create a culture of cyber security India and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.

13) To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.

14) To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

Cyber security Frameworks

Many organizations consider cyber security to be a priority. The need to implement effective cyber security strategies grows every day. Cybercriminals continuously derive more sophisticated techniques for executing attacks. This has led to the development of various frameworks meant to assist organizations in achieving robust cyber security programs. Therefore, businesses should understand the top cyber security frameworks for enhancing their security postures. Cyber security frameworks refer to defined structures containing processes, practices, and technologies which companies can use to secure network and computer systems from security threats. Businesses should understand cyber security frameworks for enhancing organizational security. The top cyber security frameworks are as discussed below:

- **ISO IEC 27001/ISO 27002**
- **NIST Cyber security Framework**
- **IASME Governance**
- **TC CYBER**
- **Fed RAMP**

Module III

Policy Catalog and Issues

A: Cyber Governance Issues:

The internet began as the Advanced Research Project Agency Network (ARPNET), a US military funded n/w designed to survive a nuclear attack.

ARPNET is become a tool for sharing information among computer science researchers in the military. In this case one of the protocols is used that is called Internet Engineering Task Force (IETF). Some of the security purposes the ARPANET is disbanded.

ICANN: Internet Corporation for Assigned Names and Numbers was created in 2000 by the National Telecommunication and Information Administration (NTIA). The resulting ICANN model is unique and its multistake holder governance model for the centralized components of the internet.

The key CS policy issue is the internet governance model and in particular the modeling of participation by world government.

One of the most unique features of the internet is that it is global shared; any internet-machine can talk to any other internet-connected machine.

Cyber user issues:

Today cyber security is the main component of the country's overall national security and economic security strategies. In India, there are so many challenges related to cybersecurity. With the increase of the cyber-attacks, every organization needs a security analyst who makes sure that their system is secured. These security analysts face many challenges related to cyber security such as securing confidential data of government organizations, securing the private organization servers, etc.

Ransomware Evolution: Ransomware is a type of malware in which the data on a victim's computer is locked, and payment is demanded before the ransomed data is unlocked. After successful payment, access rights returned to the victim. Ransomware is the bane of cybersecurity, data professionals, IT, and executives.

Blockchain technology is the most important invention in computing era. It is the first time in human history that we have a genuinely native digital medium for peer-to-peer value exchange. The blockchain is a technology that enables cryptocurrencies like Bitcoin. The blockchain is a vast global platform that allows two or more parties to do a transaction or do business without needing a third party for establishing trust.

IoT stands for Internet of Things. It is a system of interrelated physical devices which can be accessible through the internet. The connected physical devices have a unique identifier (UID) and have the ability to transfer data over a network without any requirements of the human-to-human or human-to-computer interaction. The firmware and software which is running on IoT devices make consumer and businesses highly susceptible to cyber-attacks.

Cyber Crime

Hacking: It is an illegal practice by which a hacker breaches the computer’s security system of someone for personal interest.

Unwarranted mass-surveillance: Mass surveillance means surveillance of a substantial fraction of a group of people by the authority especially for the security purpose, but if someone does it for personal interest, it is considered as cybercrime.

Child pornography: It is one of the most heinous crimes that is brazenly practiced across the world. Children are sexually abused and videos are being made and uploaded on the Internet.

Child grooming: It is the practice of establishing an emotional connection with a child especially for the purpose of child-trafficking and child prostitution.

Copyright infringement: If someone infringes someone's protected copyright without permission and publishes that with his own name, is known as copyright infringement.

Money laundering: Illegal possession of money by an individual or an organization is known as money laundering. It typically involves transfers of money through foreign banks and/or legitimate business. In other words, it is the practice of transforming illegitimately earned money into the legitimate financial system.

Cyber-extortion: When a hacker hacks someone's email server, or computer system and demands money to reinstate the system, it is known as cyber-extortion.

Cyber-terrorism: Normally, when someone hacks government's security system or intimidates government or such a big organization to advance his political or social objectives by invading the security system through computer networks, it is known as cyber-terrorism.

Module IV

Cyber Management

For a long time, cyber security management focused primarily on prevention. Prevention strategies focus on internal risks. Employees are responsible for 60% of cyber security incidents. It's up to IT pros to create a strategy that secures data but doesn't hamper users to the point where it stifles creativity and growth. The best way to do that is through employee training. Just over half of organizations do this. A training program should include employees, contractors, and vendors. The training should talk about how employee actions can put the company in a

precarious position. It won't be effective if it's done once. Employee training needs to be ongoing.

Gartner reports that 60% of cyber security management budgets will be devoted to detection and response by 2020.

To effectively implement your plan, you'll need to take these steps:

- Select your Security Controls
- Align your controls with the data you want to protect
- Prioritize which controls are implemented first
- Design your security controls
- Train employees and users affected by the controls
- Implement and monitors your security controls

Research in cyber security

Cyber is a prefix derived from the word cybernetics and has acquired the general meaning of through the use of a computer which is also termed as cyberspace. The word security in general usage is synonymous with being safe, but as a technical term security means not only that something is secure, but that it has been secured. Joining the two words together form the word cybersecurity is concerned with making cyberspace safe from threats, namely cyber threats. The information and communications technology (ICT) industry has evolved greatly over the last half century. With the advent of the internet, security becomes a major concern

Cryptographic systems: A widely used cyber security system involves the use of codes and ciphers to transform information into unintelligible data. Antimalware Software and scanners:

Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so called antimalware tools are used to detect them and cure an infected system.

Secure Socket Layer (SSL): It is a suite of protocols that is a standard way to achieve a good level of security between web browser and websites**.**

The cyber security research initiative is an attempt to define a national R&D agenda that is required to enable the country to get ahead of adversaries and produce the technologies. These futuristic technologies can protect information systems and networks. The research, development, test, evaluation and other life cycle considerations required are far reaching from technologies that secure individuals and their information to technologies that will ensure National Critical Infrastructures are much more resilient. The R&D investments recommended in this initiative must tackle the vulnerabilities of today and envision those of the future. The initiative is a platform to work together to foster R&D to evolve transformative solutions and address critical cyber security challenges, through partnerships among academics, Industry and Govt.

Module V

Government approach to cyber security policy

In recent years, the number of cyber-attacks that hit private companies and government entities has rapidly increased. The damage caused by sabotage and by the theft of intellectual property amounts to several billion dollars each year. The security community is aware of the growth of cyber threats but the current defensive approach is showing its limit to mitigate the menace from cyberspace. The cyber threats are dynamic and their attacks are asymmetric and difficult to predict. In the majority of cases victims of attacks can only find losses relating to the raids of the opponents. Law enforcement and private companies are publicly discussing the possibility to define new strategies to defend their assets from the attacks. The most plausible hypothesis is the adoption of an offensive approach to cyber security, both entities witnesses attended a Senate Judiciary Committee hearing on proposal of taking the fight to the attackers. The chapter explains government action in response to historical events and suggests areas that the

government might consider for future action. It begins with a brief historical overview of the most significant events in the past two decades that shape today's policy debates in Washington. While most of the events are clearly cyber-centric, some are not immediately obvious with respect to their contribution to the field of cyber security policy. We start this historical review with terrorist attacks against the United States in the early 1990s, and proceed through actions taken in subsequent administrations. The chapter concludes with general observations of strategy and policy that have been illustrated by the history.The U.S. Federal Government's policy attitude toward cyber security has ranged from enforcing strong standards developed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to complete ignorance of the severity.

Rise of cyber crime

Unfortunately, with technology on the rise, there's more room for cyber crime in 2018. According to the Cyber Security Breaches Survey 2018, **43% of businesses** were a victim of a cyber security breach in the last 12 months. In the U.S., the state of California lost more than **$214 million** through cyber crime alone.VPN's are being used more and more in order **to protect people's privacy online** (check the **best VPN's here**). Though, despite being made aware of the risks of clicking a link, or opening an email, the figures show that attacks are ever increasing.With evolving technology comes evolving hackers; the world are not keeping up with the fight against cybercrime.

According to **McAfee's Economic Impact of Cyber Crime** (February 2018) cyber criminals adapt at a fast pace. The scale of malicious activity across the internet is quite astounding. The figures are frightening on a monthly or yearly scale, let alone daily! **Cyber criminals are constantly finding new technologies** to target victims. With the introduction of Bitcoin, payment and transfers to/from cyber criminals is untraceable.