



Privacy and Data Protection

The Concept of Security in Cyberspace

WHAT IS CYBER SECURITY?

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.



WHY IS CYBER SECURITY IMPORTANT?

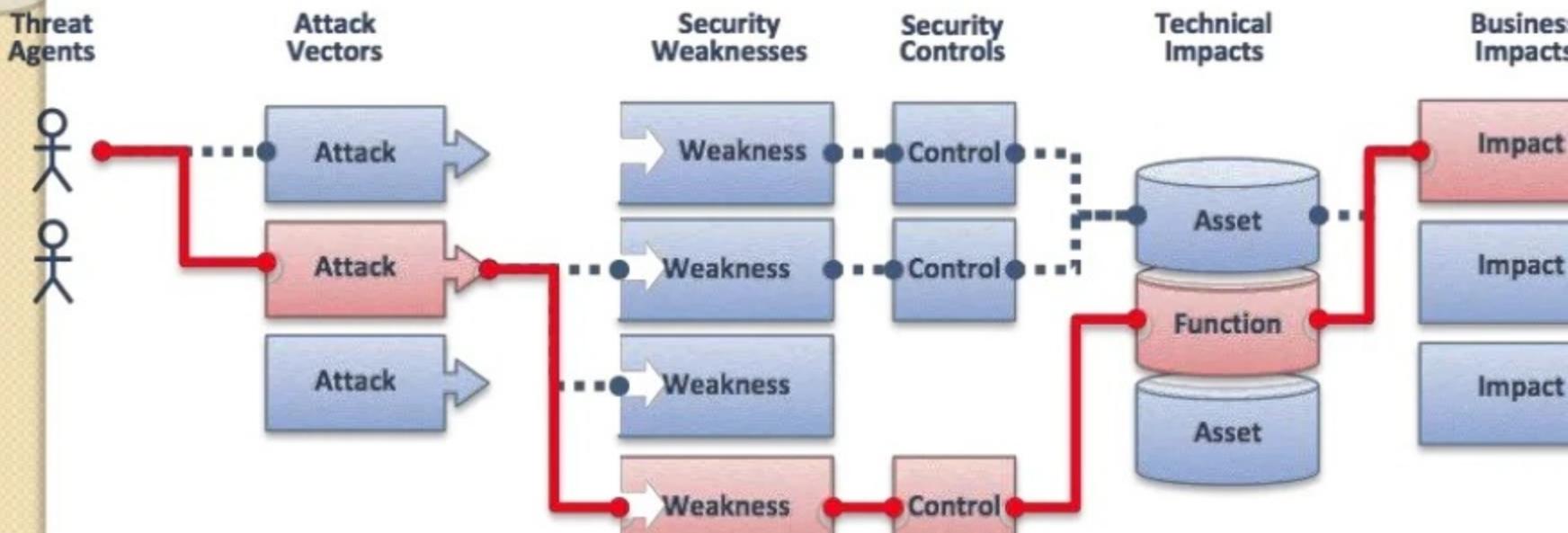
Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security.

During a Senate hearing in March 2013, the nation's top intelligence officials warned that cyber attacks and

Technological Vulnerability

- In computer security, a **vulnerability** is a weakness which allows an attacker to reduce a system's information assurance.
- Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.
- To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame

Vulnerability and risk factor models



Information Security Audit

Vulnerability Assessment and Penetration Testing Services (VAPT)

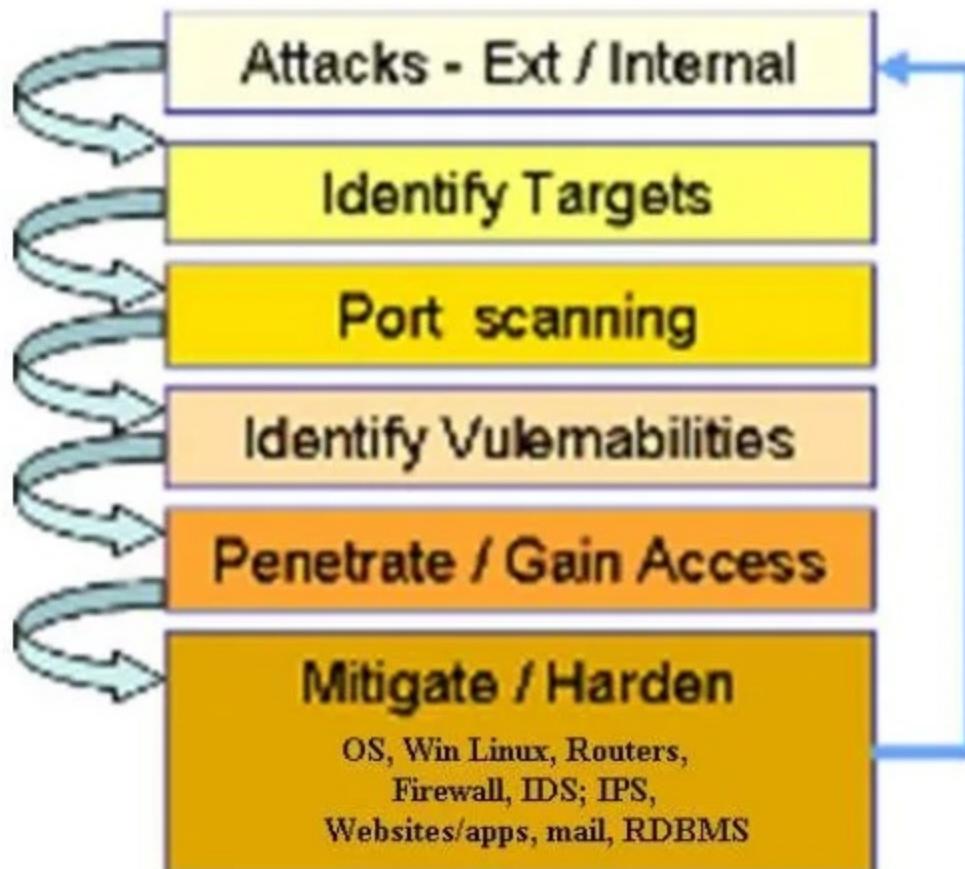
- **Vulnerability Assessments** are a process of identifying, quantifying, and prioritizing vulnerabilities in a system. A vulnerability refers to the inability of the system to withstand the effects of a hostile environment.
- **Penetration Tests** are a method of evaluating computer and network security simulating attacks on a computer system or network from external and internal



NEED OF VAPT

- VAPT is a process in which the Information & Communication Technologies (ICT) infrastructure consists of computers, networks, servers, operating systems and application software are scanned in order to identify the presence of known and unknown vulnerabilities.
- As many as 70% of web sites have vulnerabilities that could lead to the theft of sensitive corporate data such as credit card information, product IP,

Vulnerability Assessment and Penetration Testing



Data Protection Position in India

- **Data protection law in India (Present status):-**

Data Protection law in India is included in the Act under specific provisions. Both civil and criminal liabilities are imposed for violation of data protection.

(1) Section 43 deals with penalties for damage to computer, computer system etc.

(2) Section 65 deals with tampering with computer source documents.

(3) Section 66 deals with hacking with computer system.



BPOs AND THE LEGAL REGIME IN INDIA:

- Business Process Outsourcing (“BPO”) has emerged as the most challenging sector that has not only generated employment potential in India, but has also brought huge inflow of foreign exchange into the country. Today, India is home to some of the world’s leading BPO companies.
- In this context, it is becoming increasingly important to study and examine the legal regime in India pertaining to BPOs and to undertake an

- A BPO takes within its fold various elements such as finance and accounting, customer relationship management, human resources, business process, transcription, and so on. A parent company instead of performing these operations delegates them to a BPO.
- It may be an in house operation or a different company may be engaged to perform a particular task. It may be in the same country or in a different country.
- The BPO sector in India has an extremely advantageous position because of its low cost structure and large pool of skilled manpower.

Child's Privacy Online

- As a parent, you have control over the personal information companies collect online from your kids under 13.
- The Children's Online Privacy Protection Act gives you tools to do that.
- The Federal Trade Commission, the nation's consumer protection agency, enforces the COPPA Rule. If a site or service is covered by COPPA, it has to get your consent before collecting personal information and it has to honor your choices about how that information is used.



What is COPPA?

- The COPPA Rule was put in place to protect kids' personal information on websites and online services — including apps — that are directed to children under 13. The Rule also applies to a general audience site that knows it's collecting personal information from kids that age.
- COPPA requires those sites and services to notify parents directly and get their approval before they collect, use, or disclose a child's personal information. Personal information in the world of COPPA includes a



EVOLVING TRENDS IN DATA PROTECTION AND INFORMATION SECURITY:

- The legal systems which deal with them, have been forced to evolve rapidly. Though the changes in law have had to deal with a number of issues in the broad area of cyber laws, the most vibrant of those have been concerned with privacy, information security, information warfare, egovernance, e-commerce and crimes on the Internet.