BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Introduction – Part-1

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Cyber Security - Introduction

innovate achieve lead

Agenda

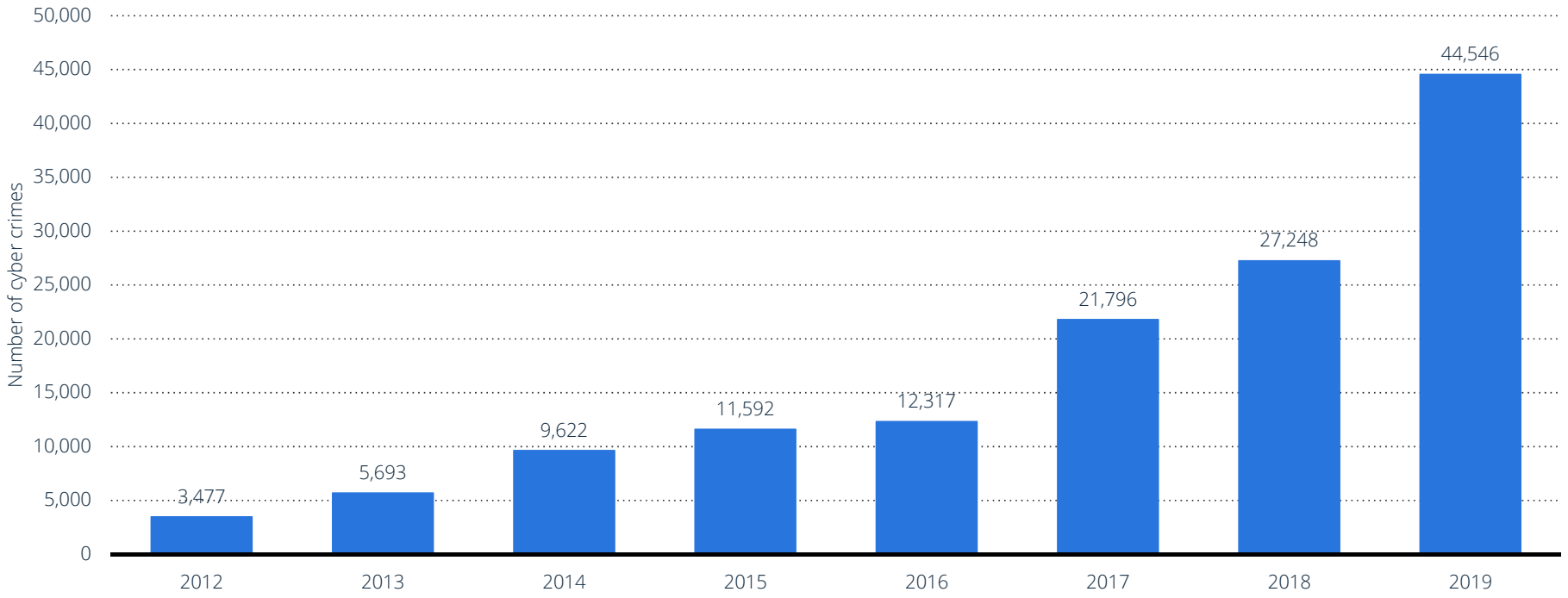
- Computer Security Concepts
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy
- Standards

Computer Security Concepts

Some Facts

Number of cyber crimes reported across India from 2012 to 2019

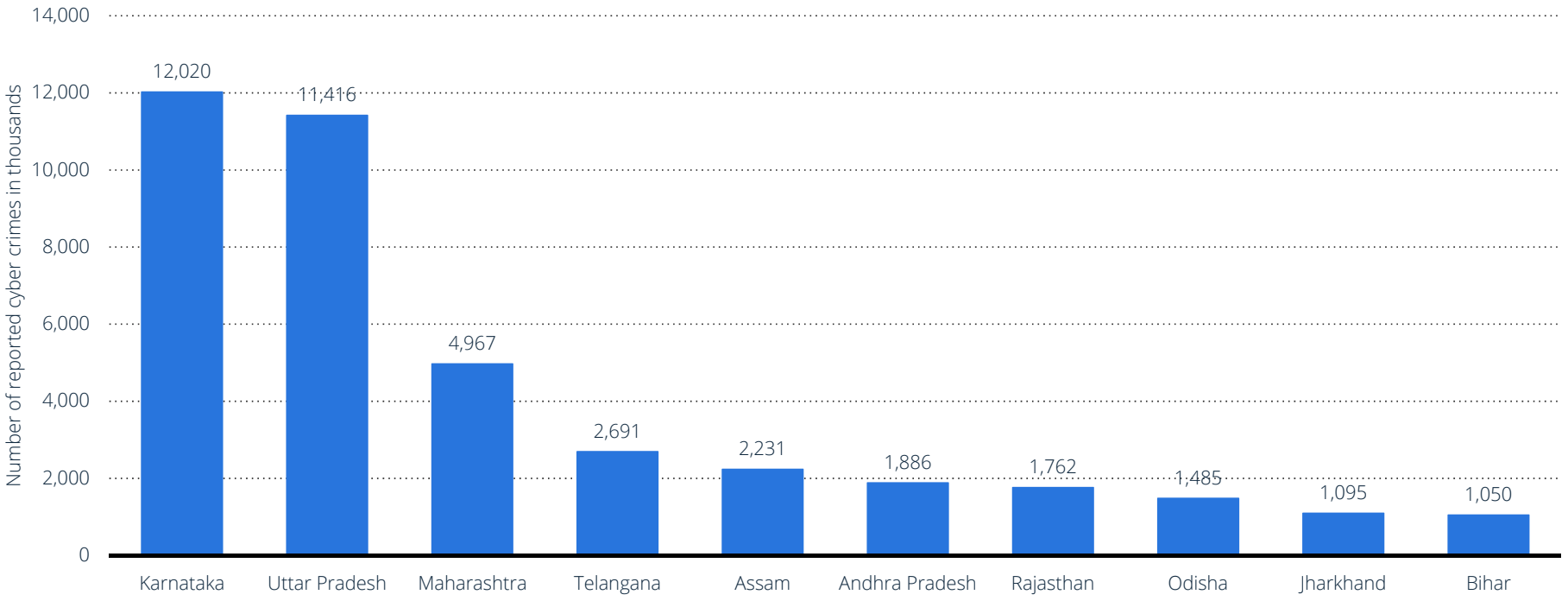
Number of cyber crimes reported in India 2012-2019



Note(s): India; 2012 to 2019; as per data provided by states and union territories.
Further information regarding this statistic can be found on page 8.
Source(s): NCRB (India); ID 309435

Number of cyber crimes reported across India in 2019, by leading state (in 1,000s)

Number of cyber crimes reported in India 2019, by leading state



Note(s): India; 2019

Further information regarding this statistic can be found on page 8.

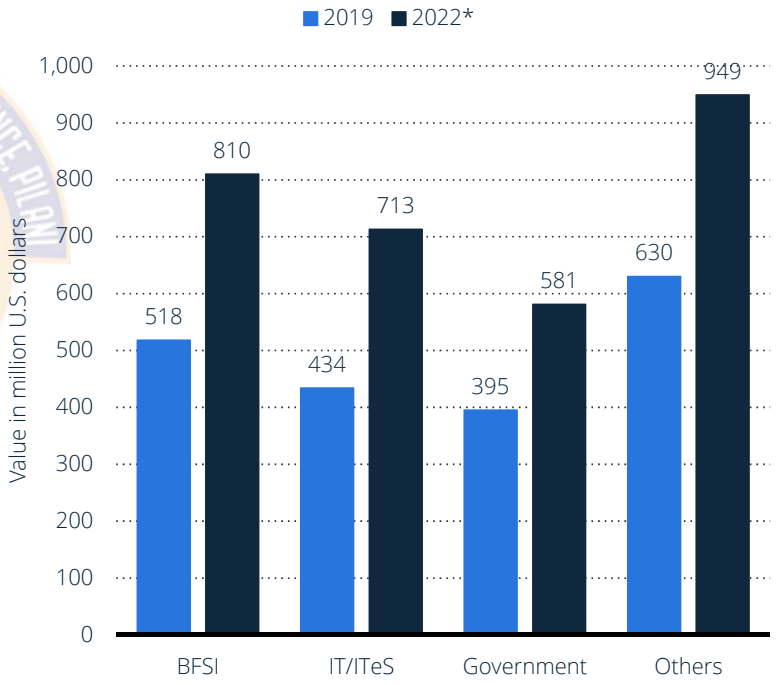
Source(s): NCRB (India); ID 1097071

Value of expenditure towards cyber security in India in 2019 and 2022, by sector (in million U.S. dollars)

innovate achieve lead

Cyber Security Expenditure in India: 2019-2022

- India's BFSI sector had the highest expenditure on cyber security
  - Over 500 million U.S. dollars in 2019
  - By 2022, this is estimated to go over $800M
- The information technology and services sector came second
  - Over $430M in 2019
  - Estimated to go over $700M by 2022
- Government sector
  - Close to $400M in 2019
  - Expected to go over $500M by 2022
- Other businesses collective expenditure
  - Over $600 Million in 2019
  - It was estimated that these expenses would reach a billion dollars by 2022

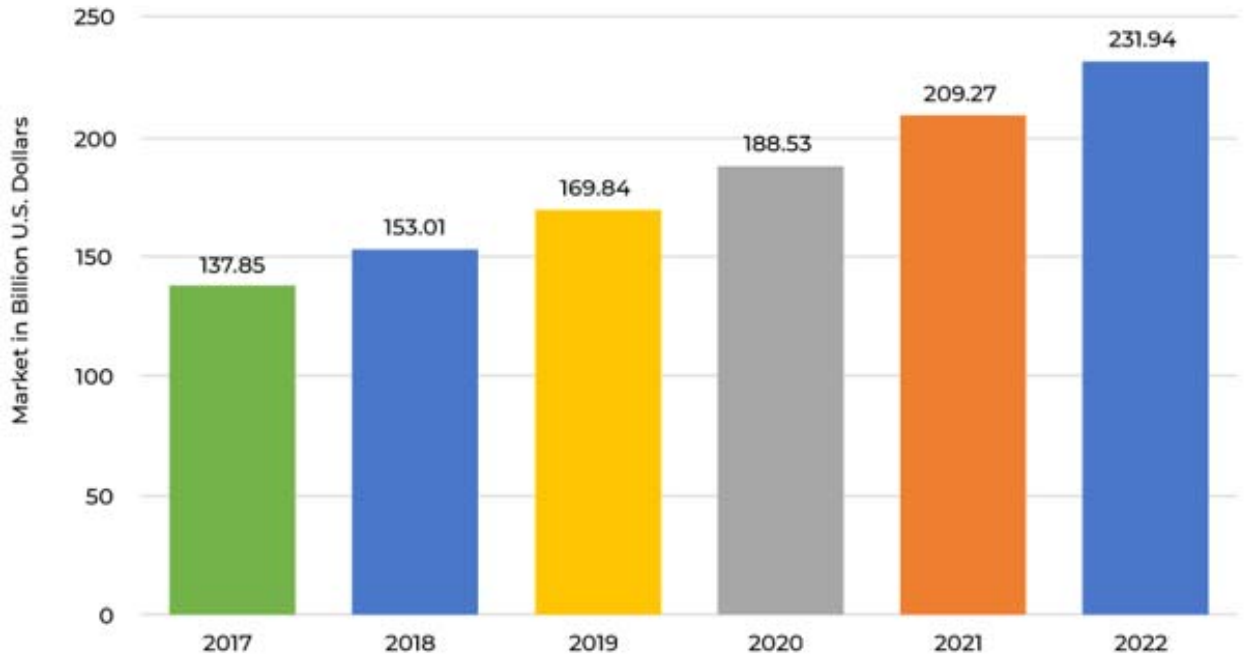


statista

Some Facts

innovate achieve lead

Scope of Cyber Security Market in India

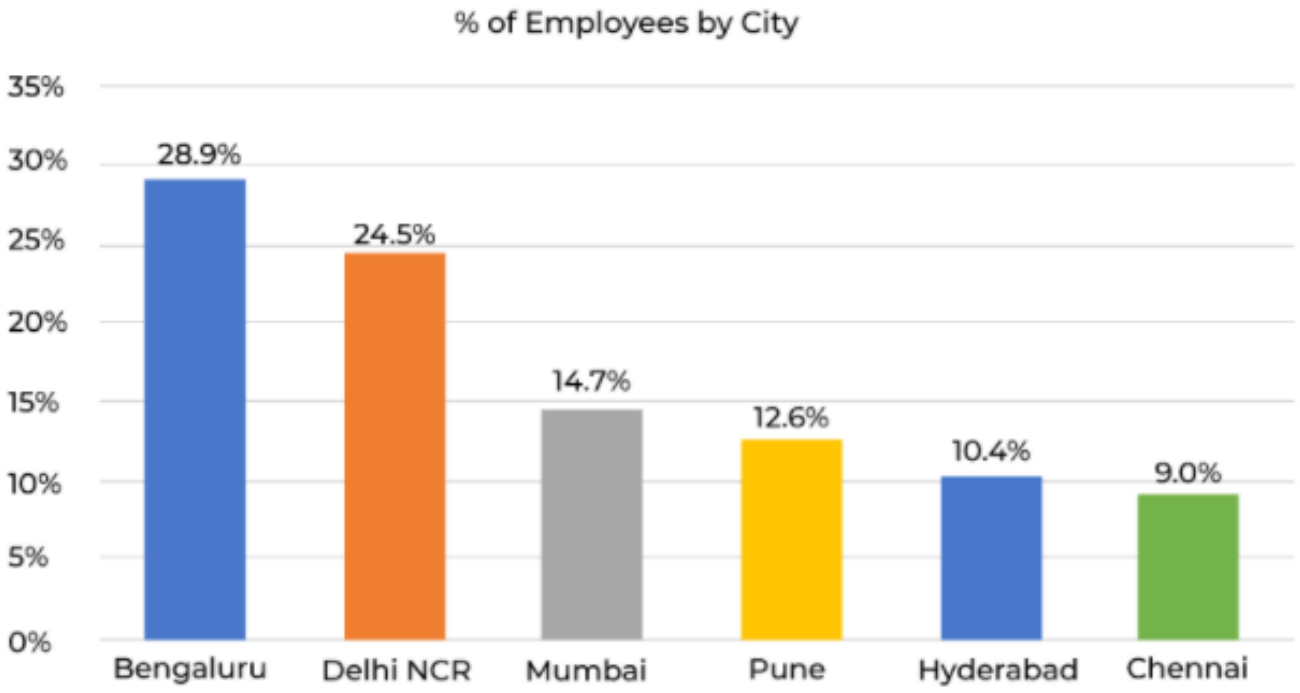


Source: State of Cyber Security in India by Jigsaw Academy & AIMResearch

Some Facts

innovate achieve lead

Cyber Security Employee Distribution: 2020

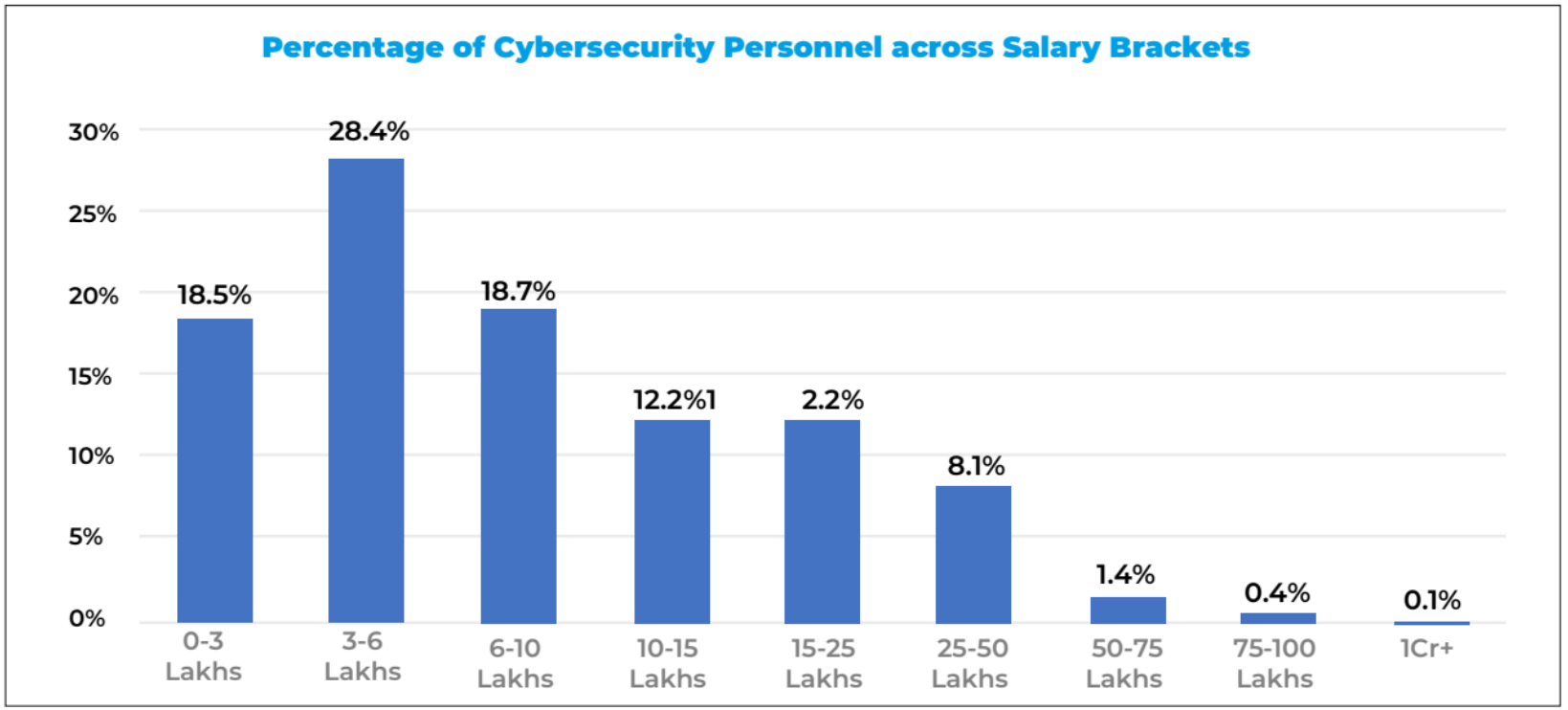


Source: State of Cyber Security in India by Jigsaw Academy & AIMResearch

Some Facts

innovate achieve lead

Cyber Security Personnel Salary Brackets: 2020

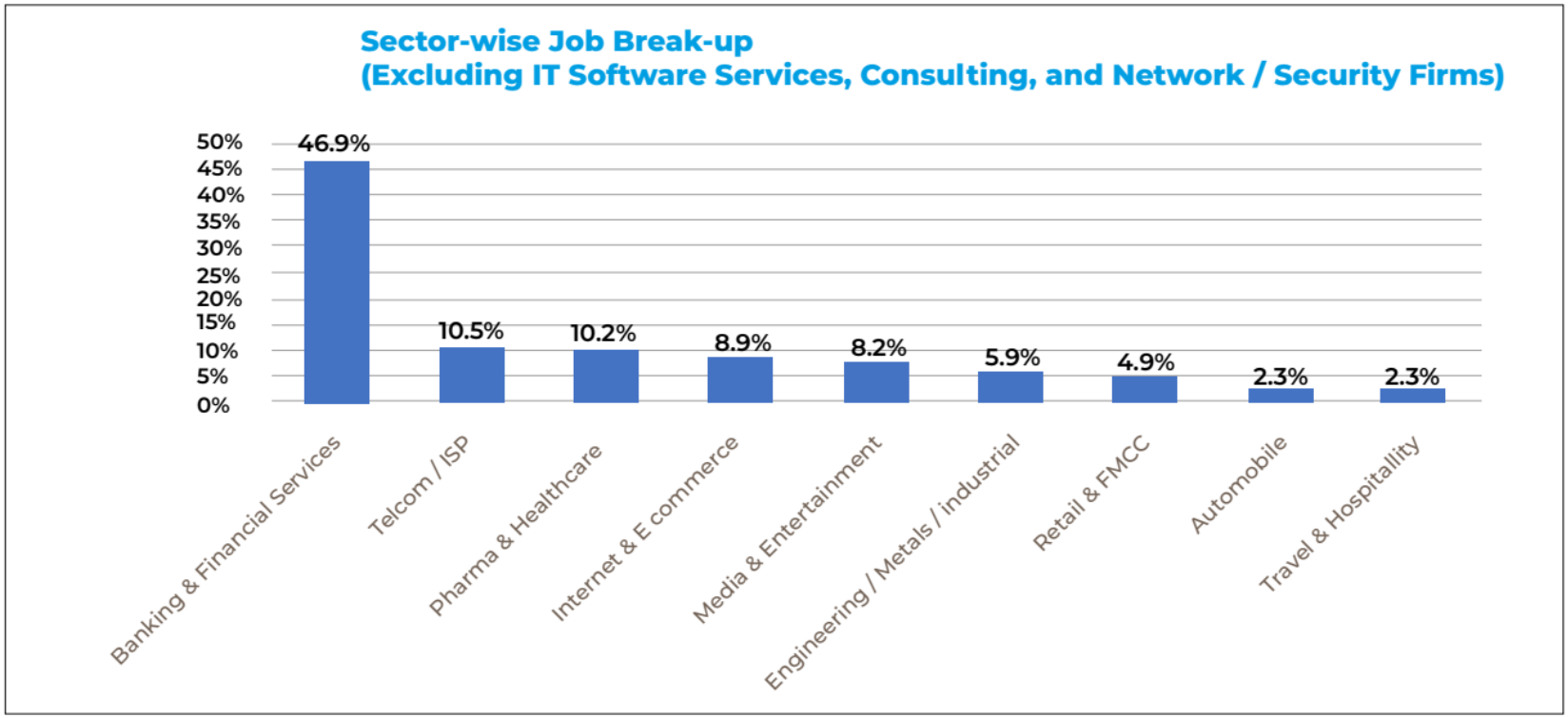


Source: State of Cyber Security in India by Jigsaw Academy & AIMResearch

Some Facts

innovate achieve lead

Cyber Security Sector-wise Job Break-up: 2020

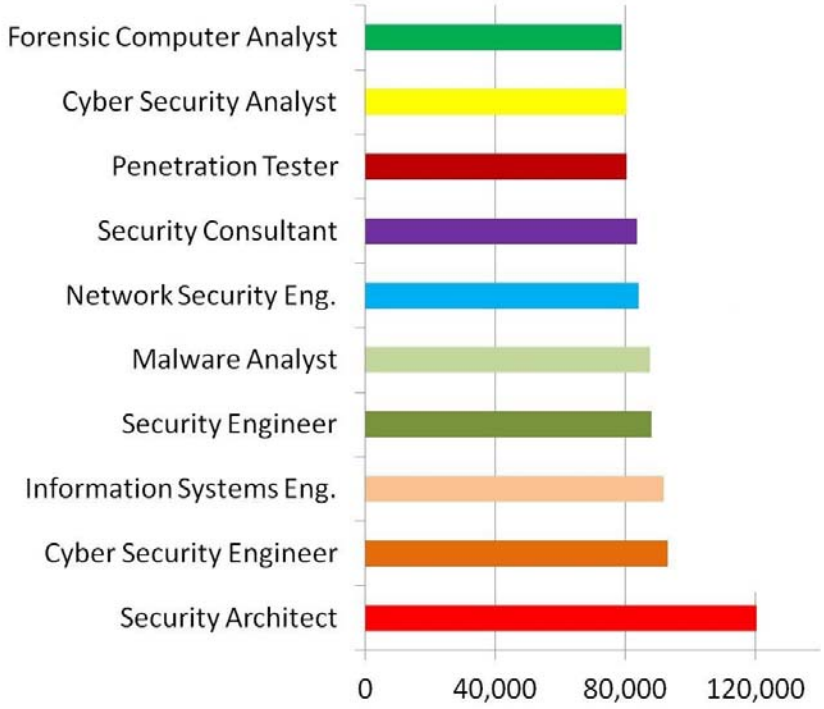


Source: State of Cyber Security in India by Jigsaw Academy & AIMResearch

Some Facts

innovate achieve lead

Cyber Security Professions and Salary: 2021



Source: State of Cyber Security in India by Jigsaw Academy & AIMResearch

A Definition of Computer Security

Computer Security Concepts

innovate achieve lead

What is Cyber Space?

- Cyberspace refers to:
  - "An interactive space comprising of digital networks that *collect*, *store*, and *manipulate* information to facilitate different forms of communication"

    -- Brian Walker

  - "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the *Internet*, *telecommunications networks*, *computer systems*, and embedded *processors and controllers*."

    -- NITI Aayog

What is Cyber Space?

- Based on the above definitions, cyberspace is a multi-layered platform that is made up of the following:
  - Information
    - Includes financial transactions, texts, and all forms of media and social media posts, etc., stored in various places.
  - Physical foundations
    - Include satellites, submarine cables, land cables, routers, and anything else that provides a pathway for communication
    - These are the transmission modules through which communication is permitted
  - People
    - Include producers and consumers of information shared in cyberspace
  - Logical building blocks
    - These are the operating systems, applications, and web browsers that allow us to interact with the physical foundations and access information online

Computer Security Concepts

What is Cyber Security?

- "the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks."
  - https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security
- "techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation."
  - https://economictimes.indiatimes.com/definition/cyber-security
- "the practice of protecting systems, networks, and programs from digital attacks."
  - https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html
- "the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.
  - https://en.wikipedia.org/wiki/Computer_security
- "the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access."
  - https://digitalguardian.com/blog/what-cyber-security

Computer Security Concepts

innovate achieve lead

What is Cyber Security?

- Data Security Council of India (DSCI)
  - A non-profit industry body on data protection in India, setup by NASSCOM®
  - Is committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy.
- According to DSCI, the term "cyber security" refers to three things:
  - A set of technical and non-technical activities and measures taken to protect computers, computer networks, related hardware and devices software, and the information they contain, including software and data, from all threats, including threats to the national security
  - The degree of protection resulting from the application of these activities and measures
  - The associated field of professional endeavor, including research and analysis, aimed at implementing and those activities and improving their quality.

Computer Security Concepts

A Definition of Computer Security

- The National Institute of Standards and Technology (NIST)
  - Is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce
  - Is responsible for establishing technology standards and metrics to be applied to the science and technology industries
- The NIST Computer Security Handbook [NIST95] defines computer security as:
  - *"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)"*

NIST: National Institute of Standards and Technology

Computer Security Concepts

A Definition of Computer Security

- This definition introduces three key elements of Computer Security:

  –Confidentiality
  –Integrity
  –Availability

  Referred as the CIA Triad

Computer Security Concepts

Key objectives of Computer Security

- **Confidentiality** covers two related concepts:
  - Data confidentiality:
    - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
    - Example:
      - SSNs and other personal information must remain confidential to prevent identity theft
      - Passwords must remain confidential to protect systems and accounts.
  - Privacy:
    - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
    - Example:
      - The Family Educational Rights and Privacy Act (FERPA) is a federal law enacted in 1974 that protects the privacy of student education records
      - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that protects patient health information from being disclosed without the patient's consent or knowledge

Key objectives of Computer Security

- **Personal Data Protection Laws in India**
  - At the moment, India does not have a specific legislation enacted primarily for data protection
  - India's regulatory mechanism for data protection and privacy is the Information Technology Act, 2000 ("the IT Act") and its corresponding Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("the IT Rules").
  - In addition to this, personal data is also protected under Article 21 of the Indian Constitution which guarantees to every citizen, the Right to Privacy as a fundamental right.
  - The Supreme Court has held in a number of cases that information about a person and the right to access that information by that person is also covered within the ambit of right to privacy

Source: https://www.rkdewan.com/articledetails.php?artid=183

Computer Security Concepts

Key objectives of Computer Security

- **Integrity** covers two related concepts:
  - Data integrity:
    - Assures that information and programs are changed only in a specified and authorized manner.
    - E.g., a user updates data fields with wrong data (phone number, address, name, etc.)
  - System integrity:
    - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
    - E.g., a bug in an application attempts to delete the wrong record.
    - E.g., a vending machine dispenses a wrong item for a certain choice pressed
- **Availability**:
  - Assures that systems are available and work promptly and service is not denied to authorized users

Computer Security Concepts

innovate achieve lead

Side Bar

- NIST has developed several standards called Federal Information Processing Standards (FIPS)
- FIPS 199 is a US Federal Government standard that establishes security categories of information systems used by the Federal Government
- FIPS 199 and FIPS 200 are mandatory security standards as required by FISMA
  - Federal Information Security Management Act of 2002
- FIPS 199 requires Federal agencies to assess their information systems in each of the categories of confidentiality, integrity and availability
  - The agencies have to rate each system as *low*, *moderate* or *high* impact in each category
  - The most severe rating from any category becomes the information system's overall security categorization
- FIPS 200 talks about minimum security requirements for Federal Information and Information Systems

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

Computer Security Concepts

innovate achieve lead

Key objectives of Computer Security

- FIPS 199 provides requirements and the definition of a loss of security in each category

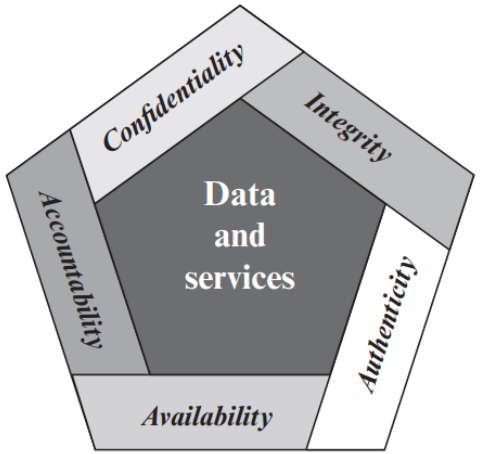
Category	Requirement	Definition of a loss of security
Confidentiality	• Preserving authorized restrictions on information access and disclosure • Includes means for protecting personal privacy and proprietary information	• A loss of confidentiality is the unauthorized disclosure of information
Integrity:	• Guarding against improper modification or destruction of information • Includes ensuring information nonrepudiation and authenticity	• A loss of integrity is the unauthorized modification or destruction of information
Availability:	• Ensuring timely and reliable access to and use of information.	• A loss of availability is the disruption of access to or use of information or an Information System

FIPS 199: Standards for Security Categorization of Federal Information and Information Systems

Computer Security Concepts

Key objectives of Computer Security

- Security experts add two additional objectives to CIA to present a complete picture
- Authenticity:
  - The property of being genuine and being able to be verified and trusted
    - Infuses confidence in the validity of a transmission, a message, or message originator
  - Verifies that users are who they say they are and that each input arriving at the system came from a trusted source
- Accountability:
  - Actions of an entity to be traced uniquely to that entity
    - Supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action
  - A security breach should be traceable to a responsible party
  - Systems must keep records of the activities to permit forensic analysis to trace security breaches or to aid in transaction disputes



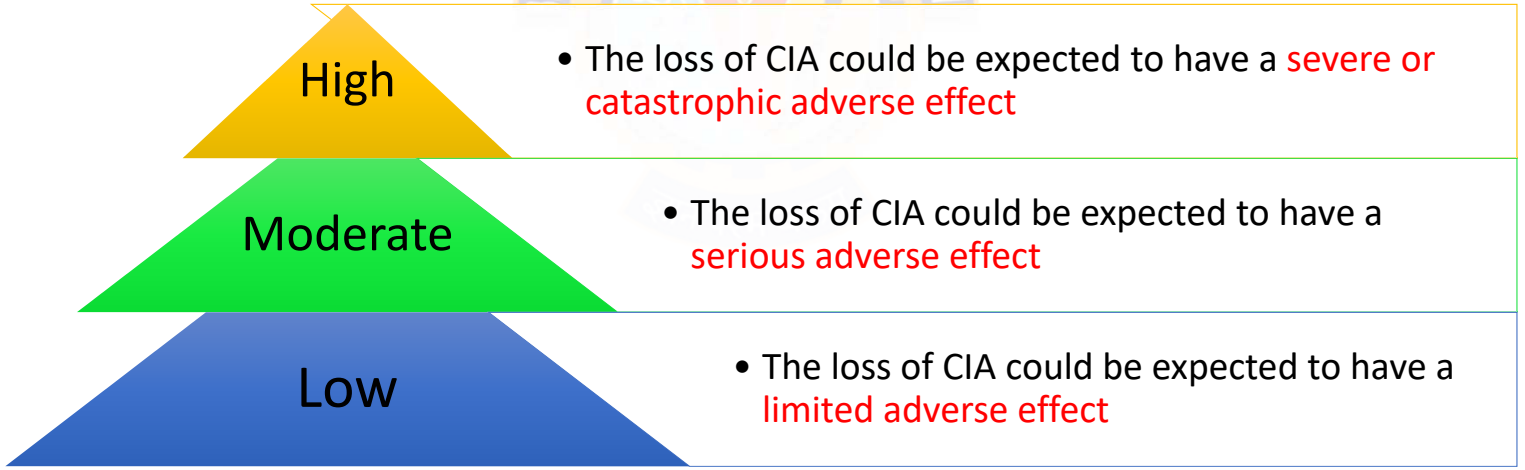
Essential Network and Computer Security Requirements

Computer Security Concepts

innovate achieve lead

CIA Triad – Levels of effects due to breach of security

- Breach of security results in a loss of C, I or A
- FIPS PUB 199 defines three levels of effects on organizational operations, organizational assets, and individuals should there be a breach of security



FIPS: Federal Information Processing Standards

Computer Security Concepts

Damages due to the loss of CIA Triad

	Breach of Security		
Effect on	**Low**	**Moderate**	**High**
Overall effect on organizational operations, assets, and individuals	Limited adverse effect	Serious adverse effect	Severe or catastrophic adverse effect
Extent and duration of degradation in mission capability	Minor	Significant	Severe
Organization is able to perform its primary functions	Yes, but the effectiveness of the functions is noticeably reduced	Yes, but effectiveness of the functions is significantly reduced	Not able to perform one or more of its primary functions
Organizational assets	Minor damage	Significant damage	Major damage
Financial loss	Minor	Significant	Major
Individuals	Minor harm	Significant harm	Severe or catastrophic harm
Loss of life or serious, life-threatening injuries	Not applicable	None	Yes

Computer Security Concepts

Loss to CIA Triad – Confidentiality – Example

Confidentiality	Example	Protected by	Accessibility
High	Student grade information	In the US, the release of such information is regulated by the Family Educational Rights and Privacy Act (FERPA)	• Grade information should only be available to students, their parents, and employees that require the information to do their job
Moderate	Student enrollment information	Also covered by FERPA	• This information is seen by more people on a daily basis • Is less likely to be targeted than grade information • Results in less damage if disclosed
Low	Directory information	Not covered by FERPA	• E.g., lists of students or faculty or departmental lists • This information is typically freely available to the public and published on a school's Web site.

Computer Security Concepts

Loss to CIA Triad – Integrity – Example

Integrity	Example	Details
High	Patient Allergy Information	• The doctor should be able to trust that the information is correct and current • Now suppose that a nurse who is authorized to access this information deliberately falsifies the data to cause harm to the hospital • The database needs to be restored to a trusted basis quickly • It should be possible to trace the error back to the person responsible • Inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability
Moderate	Web site	• Offers a forum to registered users to discuss specific topics • Either a registered user or a hacker could falsify some entries or deface the Web site • If the forum exists only for the enjoyment of the users, brings in little or no advertising revenue, and is not used for something important such as research, then potential damage is not severe • The Web master may experience some data, financial, and time loss
Low	Anonymous online poll	• Many Web sites (E.g., news organizations), run polls for their users with very few safeguards • However, the inaccuracy and unscientific nature of such polls is well understood.

Loss to CIA Triad – Availability – Example

Availability	Example	Details

High	A system that provides authentication services for critical systems, applications, and devices	• An interruption of service results in the inability for
		  • customers to access computing resources
		  • staff to access the resources they need to perform critical tasks.
		• The loss of service results into a large financial loss in lost employee productivity and potential customer loss.

Moderate	A public Web site for a university	• The Web site provides information for current and prospective students and donors • Such a site is not a critical component of the university's information system, but its unavailability will cause some embarrassment
Low	Online telephone directory lookup application	• The temporary loss of the application may be an annoyance, but • There are other ways to access the information, such as a hardcopy directory or the operator

Terminology

Terminology

Asset

- Something that users and owners wish to protect
- Can be categorized as:
  - Hardware
    - Includes computer systems, data storage, communication devices
  - Software
    - Includes operating system, system utilities, and application software
  - Data
    - Includes files, databases, security-related data such as passwords
  - Networks and Communication Facilities
    - Includes local and wide area network communication networks, bridges, routers, etc.

Terminology

innovate achieve lead

Vulnerability

- Weakness in an information system, system security procedures, or internal controls that could be exploited by a threat source
- General categories of vulnerabilities of assets (system resources)
  - Leaky system (Confidentiality issue)
    - E.g., someone who should not have access to information through network obtains such access
    - A weakness in a firewall that lets hackers get into a computer network
  - Corrupted system (Integrity issue)
    - The system does wrong things or gives wrong answers
    - E.g., A malicious macro in a Word document inserts the word "not" after some random instances of the word "is"
  - Unavailable or slow system (Availability issue)
    - Using the system or network becomes impossible or impractical

Terminology

Threat

- A threat is a set of circumstances that is capable of exploiting a vulnerability
- It is any circumstance or event with the potential to adversely impact:
  - organizational operations
  - organizational assets
  - individuals
  - organizations, or
  - the Nation

using an ICT via

  - unauthorized access
  - destruction
  - disclosure
  - modification of information, and/or
  - denial of service

Terminology

innovate achieve lead

Attack and Adversary

- Attack
  - An attack is a *threat* that is *carried out* (also called as threat action)
  - An intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system
  - Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself
    - A successful attack can lead to violation of security, or threat consequence
- Adversary (Threat agent)
  - An *individual*, *group*, *organization*, or *government* that conducts or has the intent to conduct detrimental activities
  - An *agent* carrying out the attack is referred to as an *attacker* or *threat agent*


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!