Professional Ethics

Course Code: UE17MC651

Credits: 02

P.Sreenivas, Asst.Professor, Dept. of Computer Applications

Professional Ethics

Course Objectives:

Enhance student's personal as well as professional moral, ethics and conduct.

Create awareness by providing the basic knowledge on Ethics.

Acquire knowledge about various challenges in a profession and able to apply ethical principles to resolve situations that arise in their professional lives.

Course Outcomes:

At the end of the course, the student should be able to:

Improve one's ability and judgment and refine one's behavior, decisions, and actions in performing the duty to the family, organization, and to the society.

Boost-up the interests to become an professional entrepreneur.

Perform the necessary duties to society, family and organization.

Excel in competitive and challenging environment and contribute to industry through professional careers.

Professional Ethics

Unit-1

Vulnerability.

Different types of exploits and Security Policies

Hacking and penalties of Hacking

Recent Scandals and need for Ethics

Unit-2

Micro and Macro Ethics: Ethics for IT Professionals:

Legal and ethical use of Information resources

Right to privacy act, Electronic surveillance

Ethics for IT Users: Software Piracy, Information Piracy

Inappropriate use of computing resource, In appropriate sharing of Information.

Unit-3

Responsibility and Rights Intellectual Property:

Collegiality and Loyalty, Respect for Authority, Collective Bargaining

Confidentiality, Conflicts of Interest, Occupational Crime, Professional rights,

Employee Rights, Intellectual Property Rights (IPR), Discrimination

Professional Ethics

Unit-4

Basics of Entrepreneurship:

Who are Entrepreneurs?

What is Small Business?

Rewards of Entrepreneurship, Characteristics of Successful Entrepreneurs

Varieties of Entrepreneurship

Integrity and Entrepreneurship

Unit-5

Entrepreneurship and small business:

An overview of Entrepreneurs and Entrepreneurship

Starting your Small Business

Forms of ownership, Becoming a owner,

Planning, Organizing and Managing

Obtaining the Right Financing

Professional Ethics

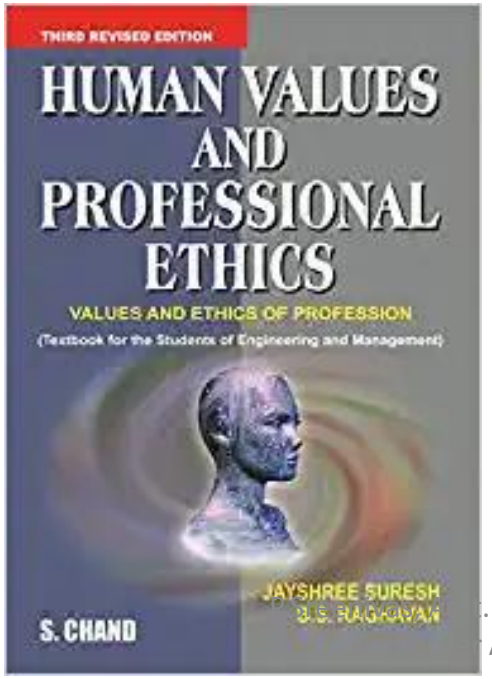
References:

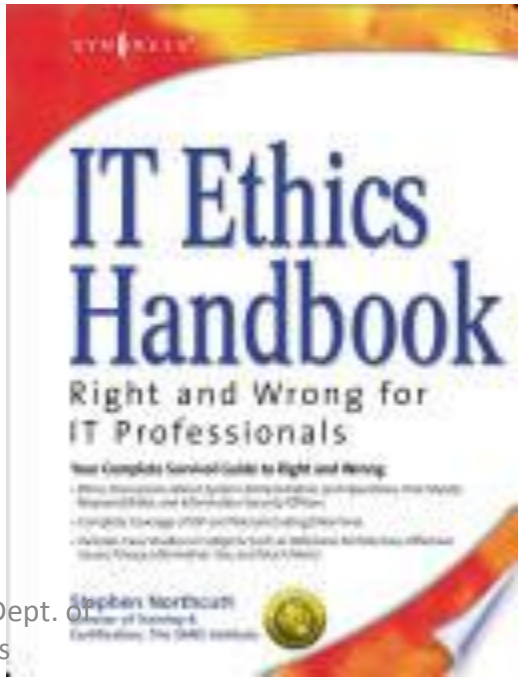
"Human Values and Professional ethics", Jayashri & B.S Raghavan, 4th Edition, S. Chand and Company

"IT Ethics Handbook", Stephen Northcut, Syngress Publishing, 2004

"Ethics for the information Age", Michael J Quinne, 7th Edition, Pearson Education, 2016

"Small Business Management -An Entrepreneurship's Guidebook", Mary Jan Byrd, McGraw Hill Publishing.





Expectations from Education- Values in Education

Education should prepare the student for:

Understanding ‘what to do’ – What is valuable, as a human being

and

Learning ‘how to do’ – skills, technology

Are both required or we can do with just one of them?

Yes! Both are important

What would be the priority between these two?

The Priority is

1. **Understanding** ‘what to do’, then → Value Education
2. **Learning** ‘how to do’ and **Doing** → Technical Education

What are Human Values???

- It is a basic moral value one has to possess to live as a human being or citizen.
- A value is defined as a principle that promotes well-being or prevents harm.
- Values are our guidelines for our success—our paradigm about what is acceptable.

Evolution of Human Values

- **Evolution of Human Values:**
- The human values evolve because of the following factors:

- 1. The impact of norms of the society on the fulfillment of the individual's needs or desires.
- 2. Developed or modified by one's own awareness, choice, and judgment in fulfilling the needs.
- 3. By the teachings and practice of Preceptors (Gurus) or Saviors or religious leaders.
- 4. Fostered or modified by social leaders, rulers of kingdom, and by law (government)

Professional Ethics

- Profession is a commitment to a designated and organized occupation by virtue of being an authority over a body of knowledge with requisite skills acquired through specialized training.

- An occupation becomes a profession when a group of people sharing the same occupation work together in a morally acceptable way with members setting and following a certain ethics code.

- A professional is a practitioner belonging to a specific profession.

Professional Ethics

- Professional ethics, as opposed to personal values and morality, is a set of ethical standards and values a practicing engineer is required to follow.

- It sets the standards for professional practice, and is only learned in a professional school or while practicing one's own profession.

(WHY PROFESSIONAL ETHICS?)

- The objectives of this course on ‘Professional Ethics and Human Values’ are:
- (a) To understand the moral values that ought to guide the profession,
- (b) Resolve the moral issues in the profession, and
- (c) Justify the moral judgment concerning the profession.
- It is intended to develop a set of beliefs, attitudes, and habits that engineers should display concerning morality.
- The prime objective is to increase one’s ability to deal effectively with moral complexity in managerial practice.

Morals and Values

What are Morals?

- Guiding principles that every human being should have.
- It is a knowledge of difference between right and wrong

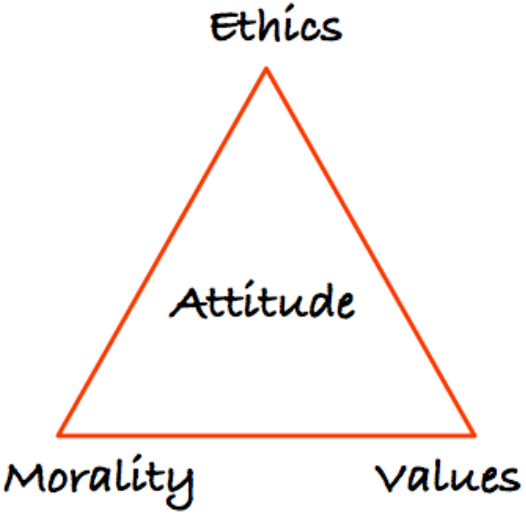
What are Values??

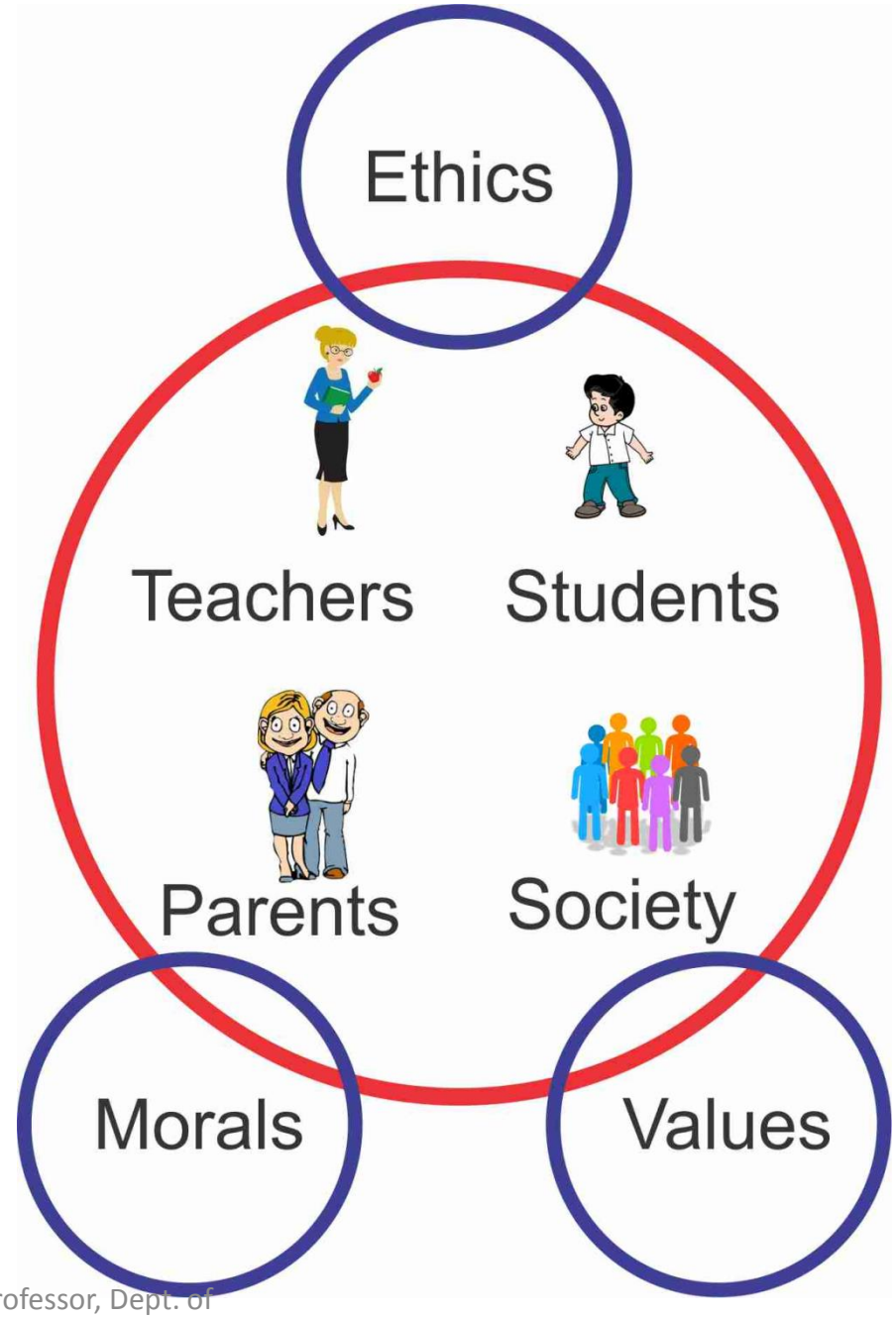
Values are individual in nature. Values are “things that have an intrinsic worth in usefulness or importance to the possessor.

Ethics, Morals, Values

- **Ethics** , derived from the Greek word *ethikos* (character), deals with the concepts of right and wrong; standards of how people ought to act.
  - Norms, Values, and The Law
- **Morals**, derived from the Latin word *moralis,* deals with manners, morals, character.
- Ethics and morals are essentially the same.
- **Values** are basic and fundamental beliefs that guide or motivate attitudes or actions

- Ancient education of India was based on guru sishya (pupil) culture emanating from high values evident in flourishing and enriching Gurukul system where Guru (teacher or Principal) stood for high morality.





Computer Crime

- A computer crime is any unlawful activity that is done using a computer.

- Computer Crimes are also called as Cyber Crimes.

The First Incident of Cyber Crime

- The first major computer crimes came into being in the 1960's when a group of hackers emerged from Massachusetts Institute of Technology.

- The first virus came into being in 1981. It was created on the Apple II operating software and was spread through floppy disk, containing the operating software.

Cyber Crime Types

1. Viruses and Worms

- Viruses are programs that attach themselves to a computer or a file. They then circulate themselves to other files and to other computers on a network.

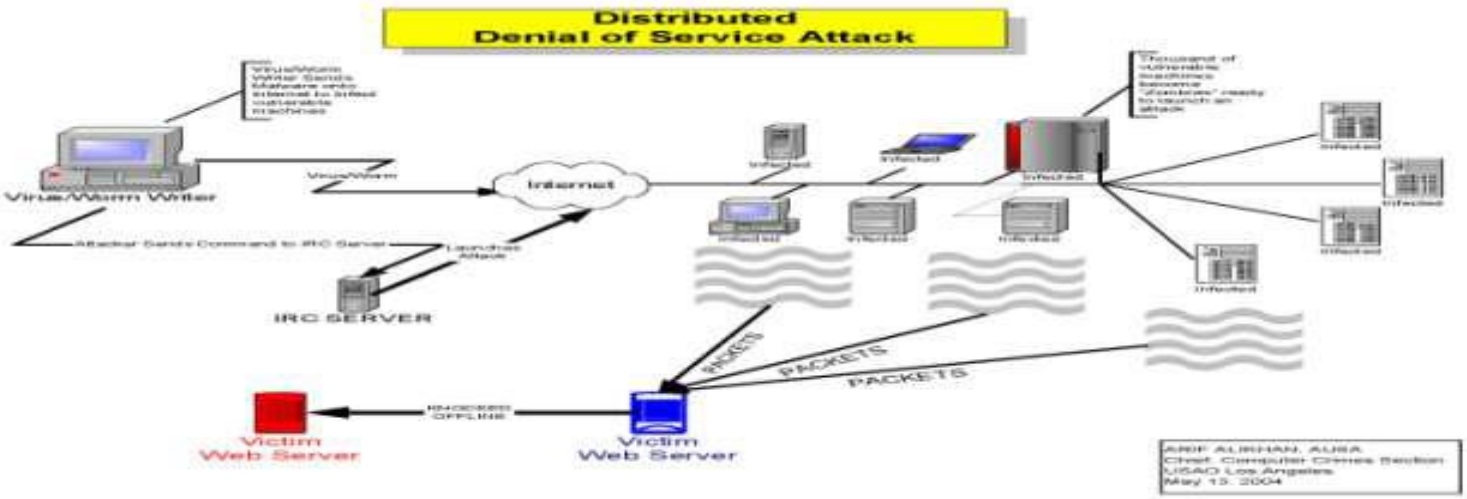
- Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

- Examples of virus and worms are

Blaster, Slammer, Nimda, Code Red, ILOVEYOU., The Morris Worm, Elk Cloner.

2. Denial-of-Service-Attacks

- These attacks occur when a person or a group of people try to prevent a
- internet site from functioning effectively either temporarily or on a long
- term basis.



3. Malware

- Malware means malicious software. It is designed to secretly access an individual's computer without his/her permission. Most malware are software's created with the intent of stealing data. Using these software's, which are usually disguised as harmless pop-ups and such, information about the users is collected without their knowledge.

4. Hacking

- Hacking is unauthorized access over a computer system, and it usually involves modifying computer hardware or software to accomplish a goal outside the creator's purpose.

5. Software Piracy

- Unauthorized copying of purchased software is called software piracy. Making copies of the software for commercial distribution, or resale is illegal.
- However software piracy is still rampant around the globe, because it is almost impossible to put an end to it.

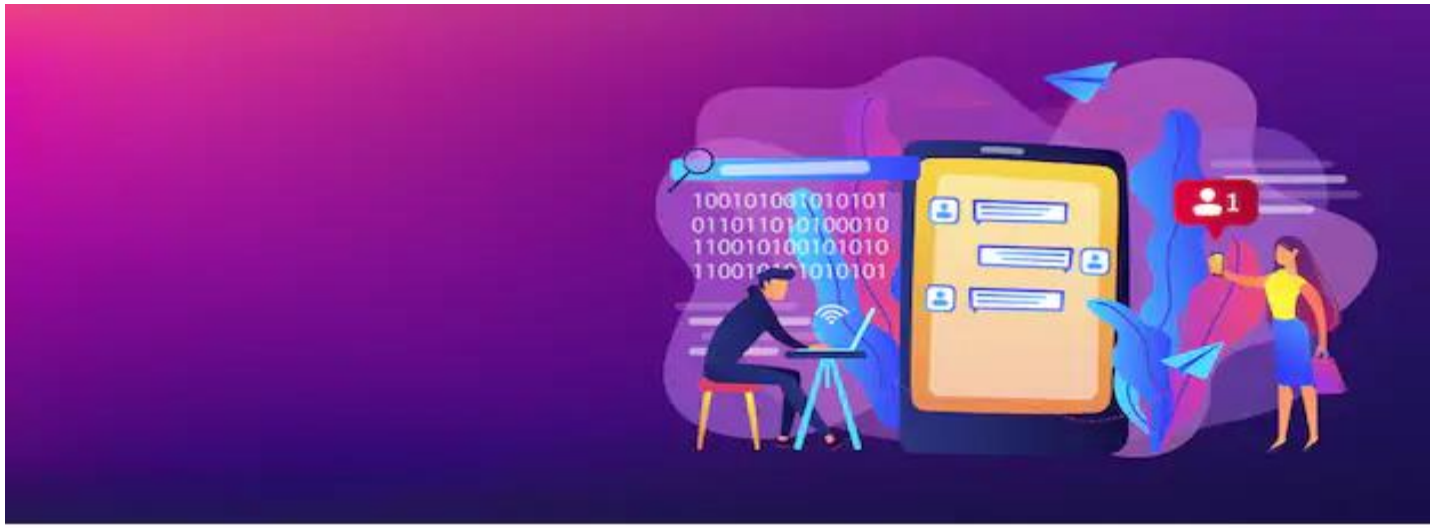
6. Fraud

- Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space.
- Some of the cases of online fraud and cheating that have come to light are those relating to credit card crimes, bank fraud, contractual crimes, internet scams, identity theft, extortion etc.

P.Sreenivas, Asst.Professor, Dept. of Computer Applications

7. Cyber stalking

- Cyber stalking involves following a person's movements across the Internet by posting threatening messages on the bulletin boards frequented by the victim, entering the chatrooms frequented by the victim, and constantly bombarding the victim with emails.



8. Obscene or Offensive Content

- Includes contents of websites that may be distasteful, obscene, or offensive in many ways. One of the major victims of this type of crime is child pornography.
- Child pornography includes sexual images involving children under puberty, puberty, and post-puberty and computer generated images that appear to involve them in sexual acts.

9. Harassment

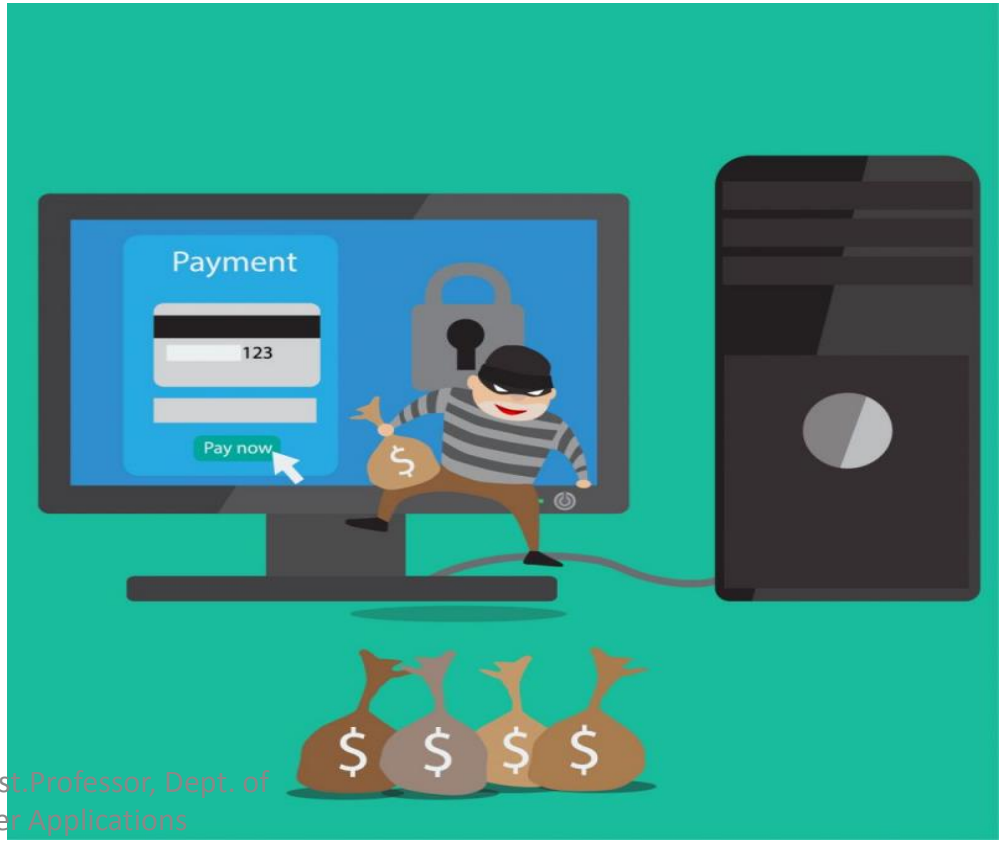
- Any comment that may be considered degratory or offensive is considered harassment. Harassment via the internet occurs in chat rooms, social networking sites, and emails.

10. Trafficking

- Trafficking may assume different forms. It may be trafficking in drugs, human beings, arms or weapons. These forms of trafficking are carried on under pseudonyms, encrypted emails, and other internet technology.

11. Computer Vandalism

- Vandalism means deliberately destroying or damaging property of another. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer, or by physically damaging a computer or its peripherals.



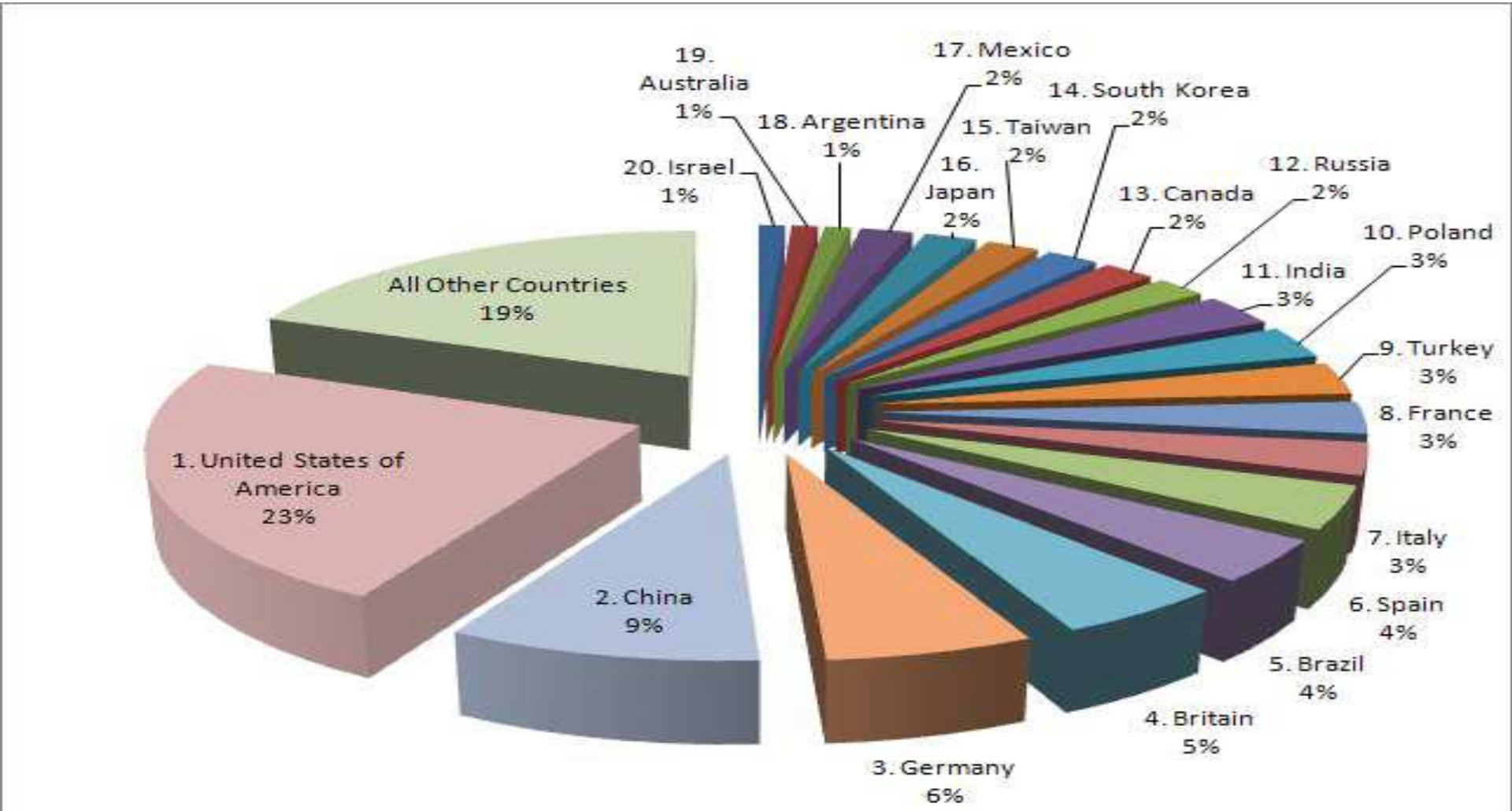
12. Spam

- The unwanted sending of bulk e-mail for commercial purposes is called spam.
- Although this is a relatively minor crime, recently new antispam laws have cropped up to restrict the sending of these e-mails.

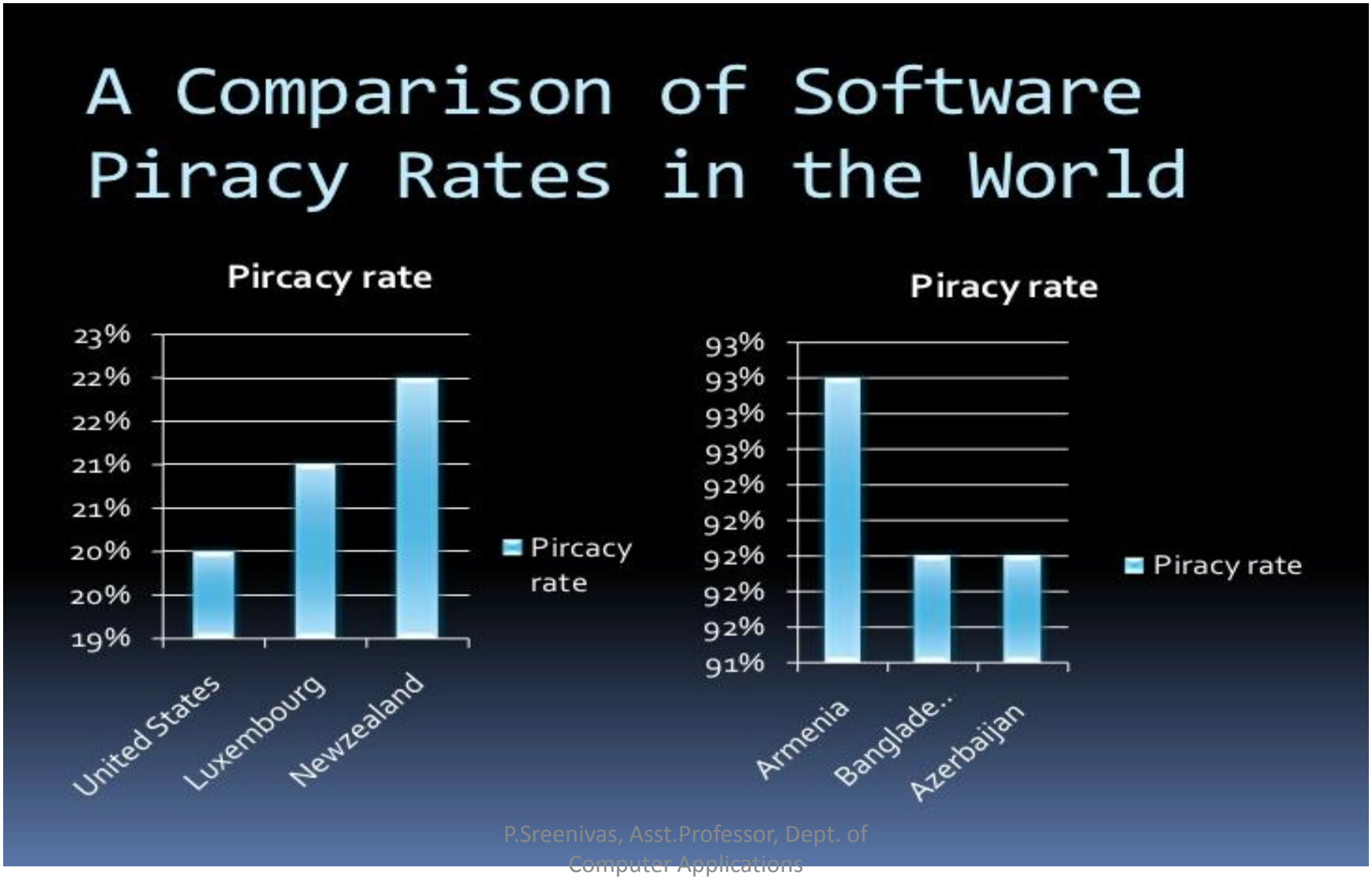
Prevention of Computer Crime

- Always use latest and updated antivirus software's to guard against virus attacks.
- Avoid sending photographs online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
- Web site owners should watch internet traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
- Use a security program that gives control over the cookies and sends information back to the site, as leaving the cookies unguarded might prove fatal.

Top 20 countries that commit the most Cyber Crimes



A Comparison of Software Piracy Rates in the World



Vulnerability

Vulnerability refers to the inability to withstand the effects of a hostile environment.

The discovery of system vulnerabilities within the software and operating system is inevitable within the information technology (IT) industry

Vulnerability

Vulnerability is a cyber-security term that refers to a flaw in a **system** that can leave it open to attack.

A **vulnerability** may also refer to any type of weakness in a computer **system** itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

When Attackers Target Vulnerabilities

Attacker creates exploits to target software vulnerability

1. Exploits may arrive via:
- Attachment to email messages
- Comproised websites
- Social networking sites

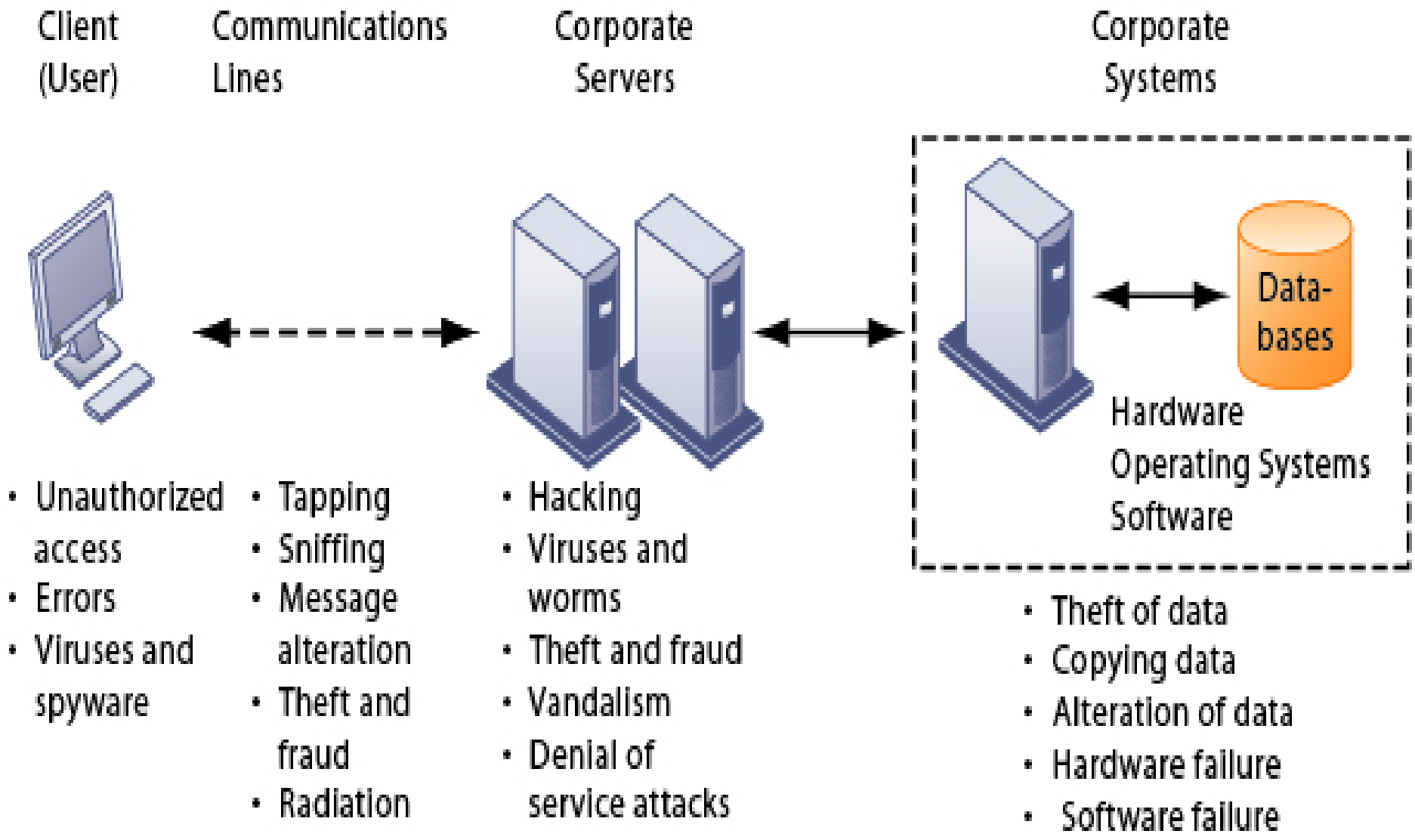
OR

2. Attacker may directly target vulnerable servers

Users are lured into executing the exploit via social engineering techniques

Exploits may drop malware onto the vulnerable system or allow attackers remote control

OR

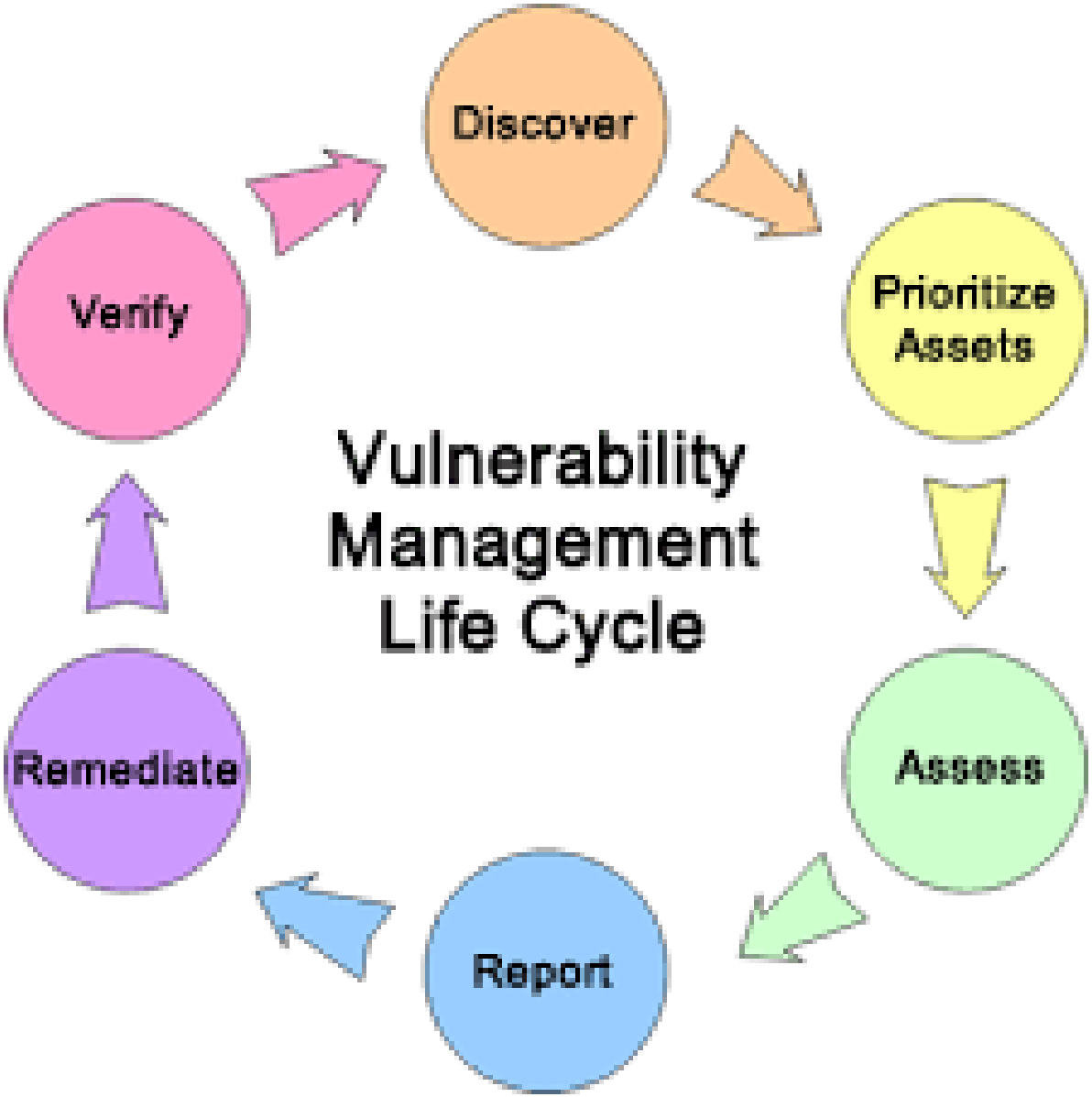

Client (User)
Communications Lines
Corporate Servers
Corporate Systems
Data-bases
Hardware
Operating Systems
Software
• Unauthorized access
• Errors
• Viruses and spyware
• Tapping
• Sniffing
• Message alteration
• Theft and fraud
• Radiation
• Hacking
• Viruses and worms
• Theft and fraud
• Vandalism
• Denial of service attacks
• Theft of data
• Copying data
• Alteration of data
• Hardware failure
• Software failure

These are the attack vectors used by attackers to trigger or reach a vulnerability in a program

41% Remote network used as attack vector

54% Local network used as attack vector

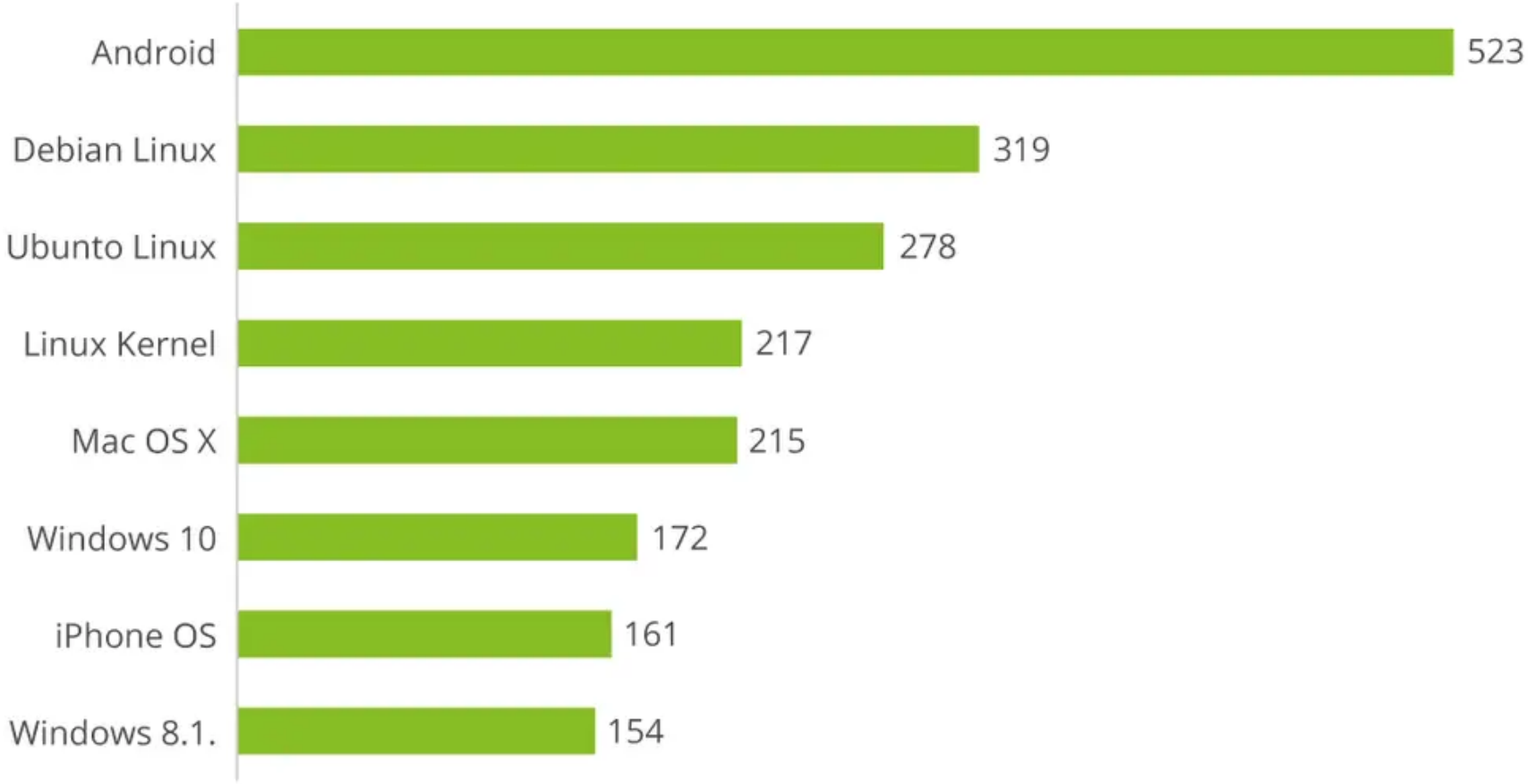
5% Local system used as attack vector


Discover
Prioritize Assets
Assess
Report
Remediate
Verify
Vulnerability Management Life Cycle

Tech Chart of the Day

Android Is The Most Vulnerable Operating System

Number of vulnerabilities by operating system in 2016*



* Vulnerability defined as a mistake in software that can be directly used by a hacker to gain access to a system/network

BUSINESS INSIDER

P.Sreenivas, Asst.Professor, Dept. of Computer Applications

Source: CVE Details

statista

Hacking

- Computer systems and the internet are characterized by **anonymity**. This haven of anonymity permits cyber crimes of various types.

- **Computer hacking** is defined as the deliberate access or **infiltration** of a computer system or program without authorization. It is also the intentional access to a computer system or program exceeding authorized access.

COMPUTER CRIMES

A person commits a “computer crime” when he or she:

- 1. accesses a computer system without authorization;
- 2. accesses or uses a computer system to obtain unauthorized computer services (including computer access, data processing, and data storage);
- 3. intentionally or recklessly disrupts, degrades, or causes disruption or degradation of computer services or denies or causes denial of computer services to an authorized user; or
- 4. intentionally or recklessly tampers with, takes, transfers, conceals, alters, or damages any equipment used in a computer system.
- It is also a computer crime to misuse computer system data.
- The punishment for committing one of these computer crimes depends on the damage caused and risk of harm created.

What is Unauthorized access or use?

UNAUTHORIZED USE OF COMPUTER OR COMPUTER NETWORK

It is a crime to use a computer or computer network without authority and with the intent to:

1. temporarily or permanently remove, halt, or disable computer data, programs, or software;

2. cause a computer to malfunction;

3. alter or erase computer data, programs, or software;

What is Unauthorized access or use?

4. create or alter a financial instrument or an electronic funds transfer;

5. cause physical injury to another's property;

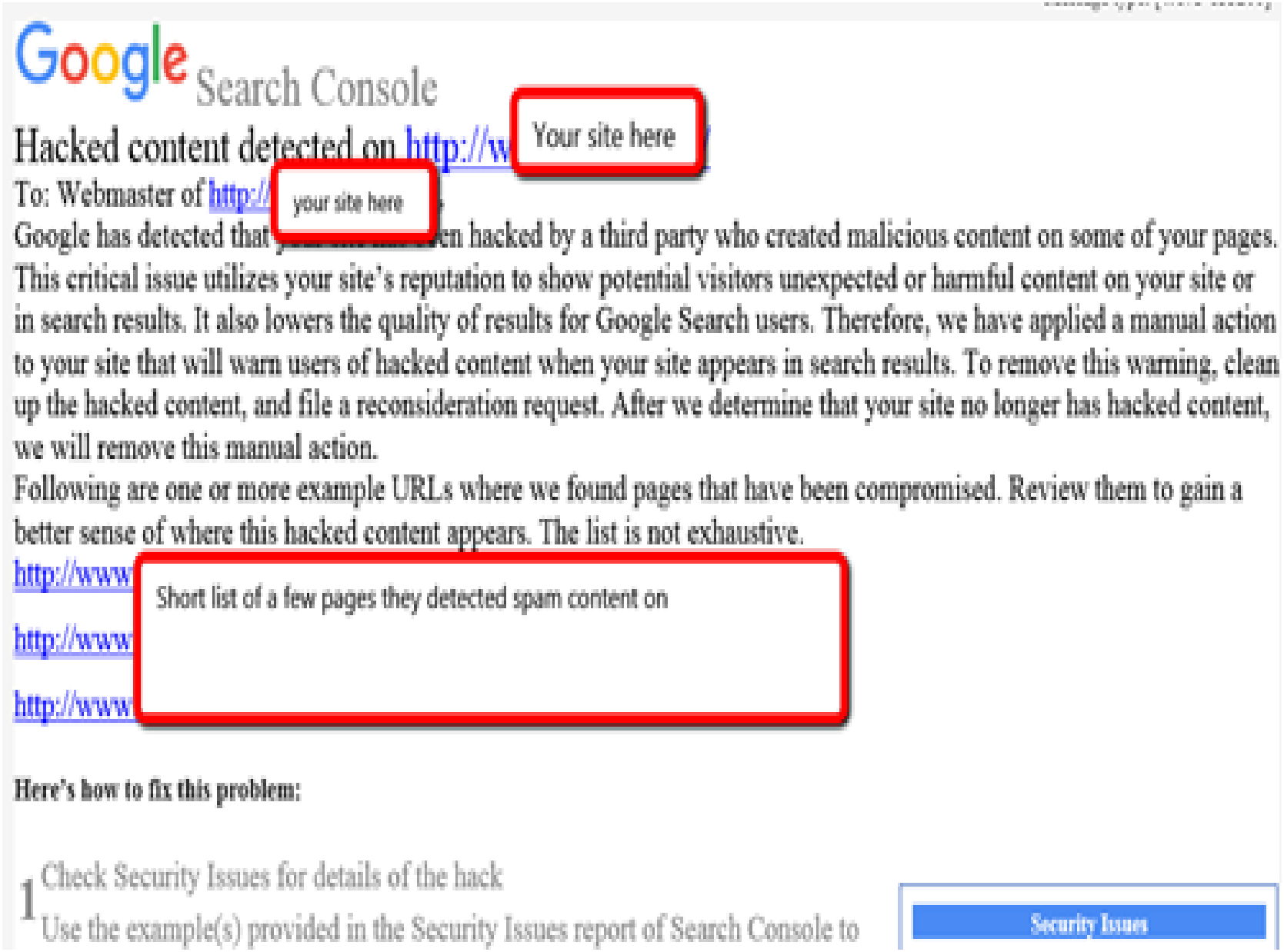
6. make or cause to be made an unauthorized copy of computer data, programs, or software residing in, communicated by, or produced by a computer or computer network;

- Depending on the circumstances, a person who hacks into another's computer could be punished by a number of generally applicable crimes.

- For example, if the hacking is done to take personal identifying information for certain purposes, it could be punishable as identity theft.

LAWS, FINES, AND PENALTIES

- Hackers, virus and worm writers could get 20 years to life in federal prison.
- Anyone who uses computers to cause death or bodily harm, such as bringing down power grids or airport control centers, can get the maximum sentence.
- The sentence is increased by 25% if they steal personal information.
- The sentence is increased by 50% if they share the stolen information.
- If posted on the Internet, sentence is doubled!


Google Search Console
Hacked content detected on http://w
Your site here
To: Webmaster of http://
your site here
Google has detected that
en hacked by a third party who created malicious content on some of your pages.
This critical issue utilizes your site's reputation to show potential visitors unexpected or harmful content on your site or in search results. It also lowers the quality of results for Google Search users. Therefore, we have applied a manual action to your site that will warn users of hacked content when your site appears in search results. To remove this warning, clean up the hacked content, and file a reconsideration request. After we determine that your site no longer has hacked content, we will remove this manual action.
Following are one or more example URLs where we found pages that have been compromised. Review them to gain a better sense of where this hacked content appears. The list is not exhaustive.
http://www
http://www
http://www
Short list of a few pages they detected spam content on
Here's how to fix this problem:
1 Check Security Issues for details of the hack
Use the example(s) provided in the Security Issues report of Search Console to
Security Issues

- Why did the site get a manual penalty?

- So what happened was, the website affected with spam is a brand blog that was previously on a separate domain from the main website. In order to consolidate content and link equity, they implemented a strategy that placed the blog on the main brand site.

- A good idea!

- The biggest problem is that the blog is managed on WordPress, and became hacked because of unsatisfactory governance.

- Yes the most popular CMS in the world has problems with hackers when not managed properly.

How the problem was fixed???

- Check Security Issues for details of the hack
- Look for other compromised pages or files on your site
- Use Fetch as Google tool to isolate the malicious content , used Screaming Frog to crawl the site for spam content and effectively isolated all of the pages on the site with the "absolute left" position.
- Remove all malicious content by checking all blog pages.
- Secure your site from any future attacks.
- Submit a reconsideration request

- Hacking earlier used to refer to a crime under section 43 of the IT Act but at the same time, ethical hacking or better known as white collar hacking was considered legal.

- Ethical hacking is also being taught by various professionals at schools and colleges. So a need was felt to differentiate between good and bad hacking. Under the amendment IT Act in 2008, the word ‘hacker was removed from the act.

What is Ethical Hacking???

- *Ethical hacking is a branch of study where computer security experts (ethical hackers/white hat hackers) find the vulnerabilities and weaknesses of a system with the permission of the owner of the system who is responsible for fixing of vulnerability.*

- *So it can be called a good hacking which finds out any probable way to hack the system and fixes it before it is hacked by black hat hackers.*

- Ethical hacking is also known as penetration testing, intrusion testing, or red teaming but it is not only limited to penetration testing.

- If hacking is offensive, ethical hacking is defensive.

- Need of Ethical Hacking
  - *India is ranked third among countries which are facing highest number of cyber threats as per security software firm Symantec*. The same research also ranked second in terms of targeted attacks.

- In 2017, 5.09% of global threats detected were in India, slightly less than 5.11% in 2016. The U.S. (26.61%) was most vulnerable to such attacks, followed by China (10.95%), according to ‘Internet Security Threat Report’.

- The global threat ranking is based on eight metrics — malware, spam, phishing, bots, network attacks, web attacks, ransomware and cryptominers.

In India- The Laws

- *Hacking, a cyber crime covered under the Information and Technology Act, 2002.*

- The Information and Technology Act, 2000 (IT Act) covers all types of cyber crime committed in the country including hacking.

- Section 43 and section 66 of the IT Act cover the civil and criminal offenses of data theft or hacking respectively.

- Under section 43, a simple civil offense where a person without permission of the owner accesses the computer and extracts any data or damages the data contained therein will come under civil liability.

- Section 66B covers punishment for receiving stolen computer resource or information. The punishment includes imprisonment for one year or a fine of rupees one lakh or both.

Incidents of Hacking

- There have been numerous hacking attacks on Indian government websites where state government websites or defense websites have been hacked.

- Principal Controller of defense accounts website was hacked due to which defense officials could not access their salary information.

- The government, to reduce hacking of precise work, has agreed to the proposal of DEITY, which is the department of information and technology to stop using popular email ids for official purpose and has sanctioned a budget of Rs. 100 cores to safeguard the data.

- In the infamous case of Amit Tiwari, who was a global hacker, he has hacked more than 950 accounts since 2003 and was caught by the police only in 2014. This shows the lack of evidence and the difficulty in arresting a hacker.

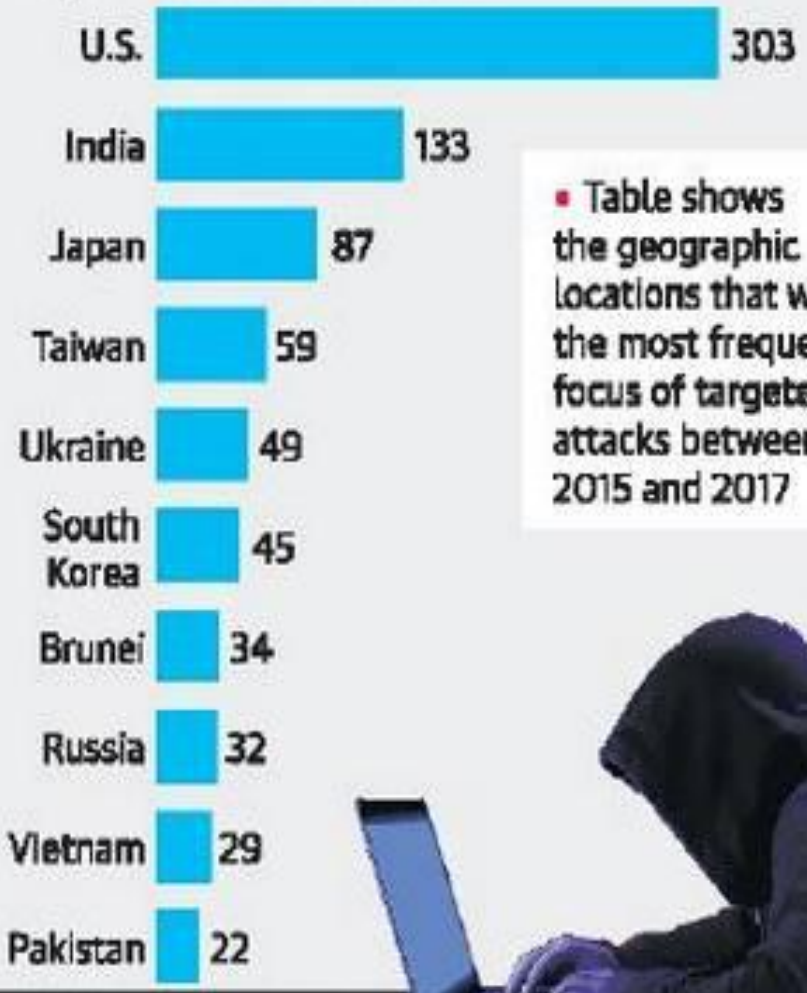
Pune-based global hacker Amit Tiwari arrested

Engineering dropout Amit Vikram Tiwari, 32, compromises 950 foreign email accounts and 171 Indian; he was nabbed in 2003 as well.

Cyber victims

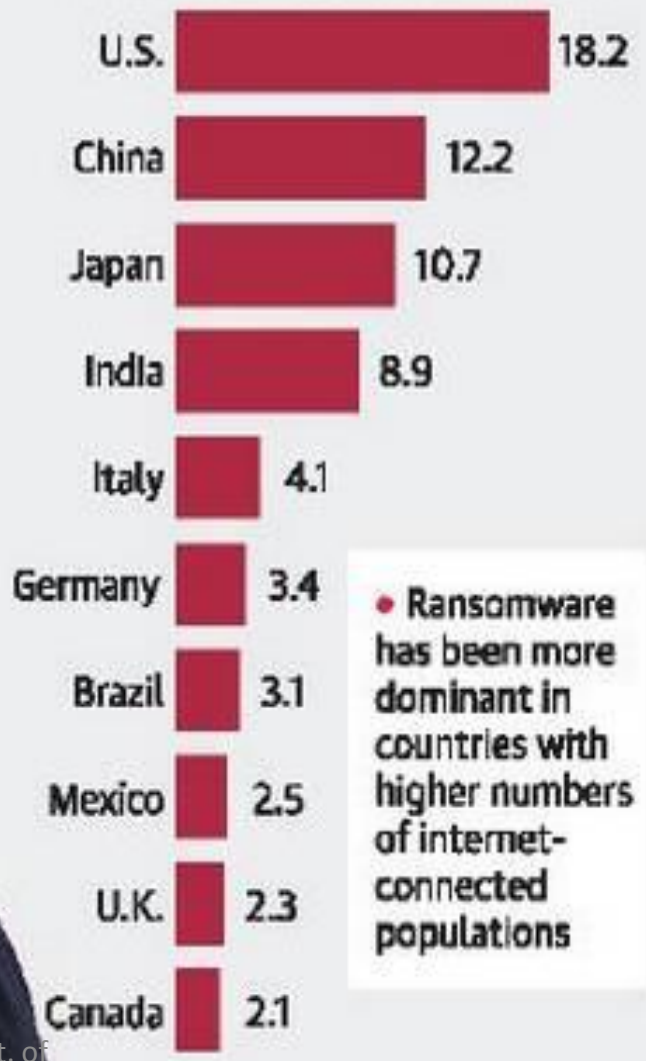
After the United States, India was most affected by targeted attacks between 2015 and 2017 says Symantec

Targeted attacks (2015-2017)



- Table shows the geographic locations that were the most frequent focus of targeted attacks between 2015 and 2017

Ransomware detections (% share)



- Ransomware has been more dominant in countries with higher numbers of internet-connected populations

Real Scandals and top data breaches

- **1. Yahoo**
- **Date:** 2013-14
- **Impact:** 3 billion user accounts
- **Details:** In September 2016, the once dominant Internet giant, while in negotiations to sell itself to Verizon, announced it had been the victim of the biggest data breach in history, likely by “a state-sponsored actor,” in 2014.

- The attack compromised the real names, email addresses, dates of birth and telephone numbers of 500 million users. The company said the "vast majority" of the passwords involved had been hashed using the robust bcrypt algorithm.

- The breaches knocked an estimated $350 million off Yahoo’s sale price. Verizon eventually paid $4.48 billion for Yahoo’s core Internet business.

- **2. Marriott International**
- **Date:** 2014-18
- **Impact:** 500 million customers
- **Details:** In November 2018, Marriott International announced that cyber thieves had stolen data on approximately 500 million customers.

- The breach actually occurred on systems supporting Starwood hotel brands starting in 2014. The attackers remained in the system after Marriott acquired Starwood in 2016 and were not discovered until September 2018.

- **3. Adult Friend Finder**

- **Date:** October 2016
- **Impact:** More than 412.2 million accounts
- **Details:** The FriendFinder Network, which included casual hookup and adult content websites like Adult Friend Finder, Penthouse.com, Cams.com, iCams.com and Stripshow.com, was breached sometime in mid-October 2016. Hackers collected 20 years of data on six databases that included names, email addresses and passwords.

4. eBay

- **Date:** May 2014
- **Impact:** 145 million users compromised
- **Details:** The online auction giant reported a cyberattack in May 2014 that it said exposed names, addresses, dates of birth and encrypted passwords of all of its 145 million users.

- The company said hackers got into the company network using the credentials of three corporate employees, and had complete inside access for 229 days, during which time they were able to make their way to the user database.

5. Target Stores

- **Date:** December 2013
- **Impact:** Credit/debit card information and/or contact information of up to 110 million people compromised.
- **Details:** The breach actually began before Thanksgiving, but was not discovered until several weeks later.

- The retail giant initially announced that hackers had gained access through a third-party HVAC vender to its point-of-sale (POS) payment card readers, and had collected about 40 million credit and debit card numbers.

6. TJX Companies, Inc.

- **Date:** December 2006
- **Impact:** 94 million credit cards exposed.
- **Details:** There are conflicting accounts about how this happened. One supposes that a group of hackers took advantage of a weak data encryption system and stole credit card data during a wireless transfer between two Marshall's stores in Miami, Fla. The other has them breaking into the TJX network through in-store kiosks that allowed people to apply for jobs electronically.

- Albert Gonzalez, hacking legend and ringleader of the Heartland breach, was convicted in 2010 of leading the gang of thieves who stole the credit cards, and sentenced to 20 years in prison, while 11 others were arrested. He had been working as a paid informant for the US Secret Service, at a $75,000 salary at the time of the crimes

7. Uber

- **Date:** Late 2016
- **Impact:** Personal information of 57 million Uber users and 600,000 drivers exposed.

- The company learned in late 2016 that two hackers were able to get names, email addresses, and mobile phone numbers of 57 users of the Uber app. They also got the driver license numbers of 600,000 Uber drivers.

- No other data such as credit card or Social Security numbers were stolen. The hackers were able to access Uber's GitHub account, where they found username and password credentials to Uber's AWS account. Those credentials should never have been on GitHub.

8. Sony's PlayStation Network

- **Date:** April 20, 2011
- **Impact:** 77 million PlayStation Network accounts hacked; estimated losses of $171 million while the site was down for a month.
- **Details:** This is viewed as the worst gaming community data breach of all-time. Of more than 77 million accounts affected, 12 million had unencrypted credit card numbers. Hackers gained access to full names, passwords, e-mails, home addresses, purchase history, credit card numbers and PSN/Qriocity logins and passwords.

- Still many more… (https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html)

Data breaches/Hacks in India

The Big Phone Hack

- *The recent WhatsApp breach targeting dissident Indians with spyware underlines the possibility of a wider vulnerability.*

- Late in the evening on October 28, 2019, Delhi-based freelance journalist Rajeev Sharma received a phone call. The caller identified himself as John Hilton, a researcher from CitizenLab, a Canada-based Internet Research agency. Sharma was warned that his phone had been under surveillance for two weeks until May 2019. He was not alone. It turns out that the phones of several dozen Indian journalists, lawyers and activists were hacked using an invasive Israeli-developed malware.

- LinkedIn was hacked in the year 2016 and some 6.5 million accounts are said to have been affected. However, four years later, in May 2016, the company said that many more users were affected by the breach.

- In September 2016, email and password data of 68 million Dropbox users was found selling on the darknet marketplace. The dataset was claimed to be part of a 2012 hacking attack. The company sent out emails to affected users asking them to reset their passwords. According to Motherboard website, in all the details of 68,680,741 accounts were stolen.

- Facebook is facing one of the biggest scandals in its history. The company is under fire for 'improperly sharing' user's personal data with a UK-based company called Cambridge Analytica. The data is said to have been used later to influence US election results.

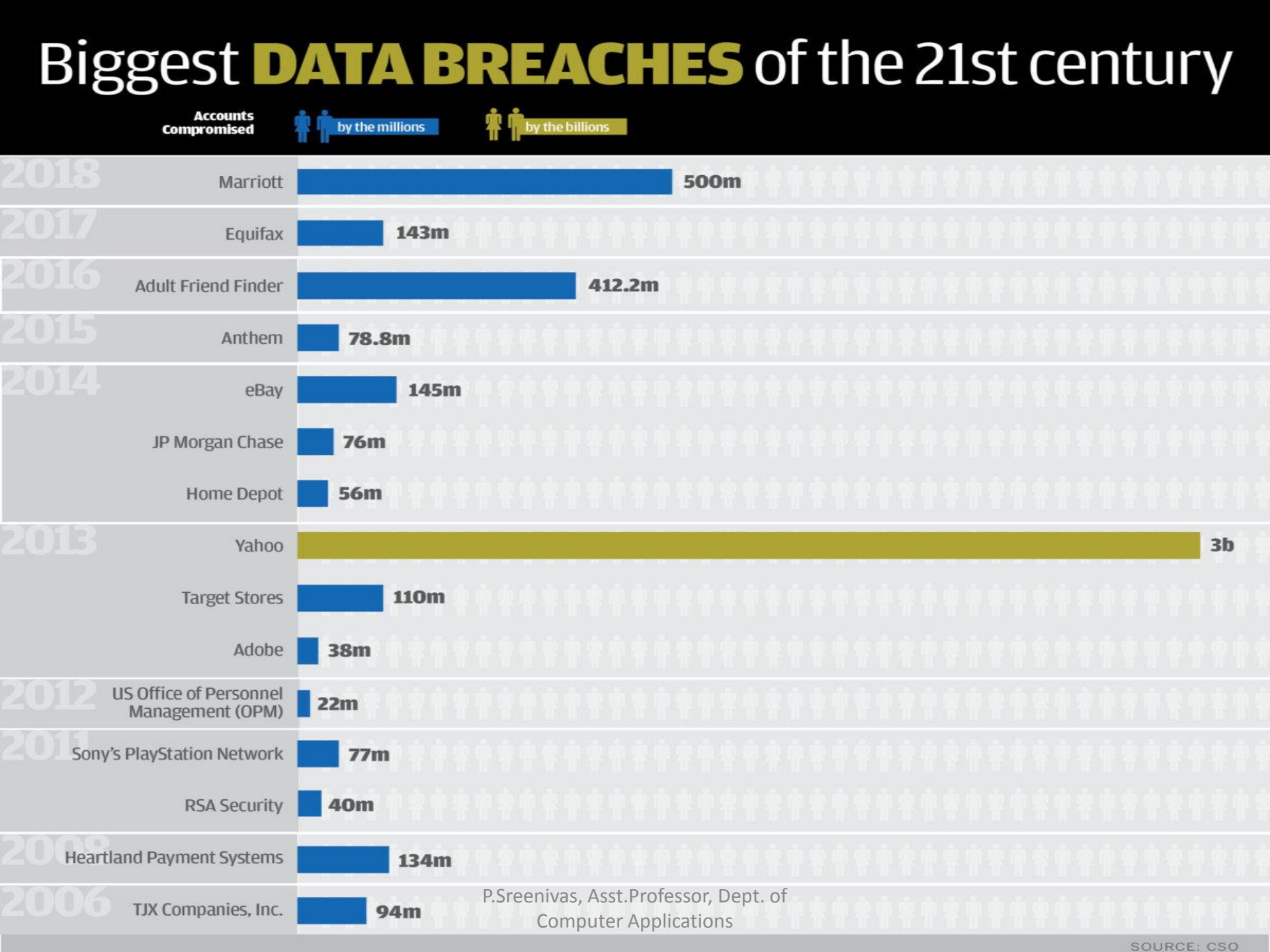
- In the year 2018, Facebook claimed that in all some 87 million users have been affected by the data breach. As for India, as per the social networking company, the figures stand at approximately 562,120 people.

- Restaurant app Zomato suffered a major security breach in May 2017 when data of some 17 million users was stolen.

- Hackeread.com claimed that a user by the name of "nclay" claimed to have hacked Zomato and was offering data of some 17 million registered Zomato users on darkweb marketplace.

- Zomato had acknowledged the hacking attack, however, claimed that no payment information or credit card data was stolen/leaked.

Biggest DATA BREACHES of the 21st century



P.Sreenivas, Asst.Professor, Dept. of Computer Applications