International Interdisciplinary Virtual Conference on
'Recent Advancements in Computer Science, Management and Information Technology'
International Journal of Scientific Research in Computer Science,
Engineering and Information Technology| ISSN : 2456-3307 (www.ijsrcseit.com)

Ethical Issues and Social Responsibilities

Prof. H. S. Wadhone[1]
[1]Assistant Professor
Smt R. D. G. College for Women Akola, Maharashtra, India

ABSTRACT

The Social and Ethical Responsibilities of Computing (SERC) is facilitating the development of responsible "habits of mind and action" for those who create and deploy computing technologies and fostering the creation of technologies in the public interest.

It is also discovered that we are vulnerable to their malfunction and misuse, creating problems such as computer crime, software theft, hacking, viruses, and invasionsof privacy, an over- reliance on intelligent machines and workplace stress, each of which has created one or more ethical dilemmas for the computer profession

Keywords: Software theft, Netiquette, Ethical Dilemmas, ransomware

I. INTRODUCTION

The digital computer is a key technology of the modern era and has been central and essential to key operations in modern industrial society, including manufacturing, transport and distribution, government, the military, health services, education and research. And their impact will most likely increased over the next century.

Most technological problems these days get blamed on computers including power supplies failing, phone systems going down, air traffic controls seizing up, traffic lights on the blink. Also computers get blamed for mistakes made by utilities, governmental agencies, credit-checking bureaus, the police, etc.

New social problems caused by computerization

Computer crime

- New technology brings with it new opportunities for crime, but in many ways, computers and computer networks have left many open doors for criminal to enter.
- People are stealing or doctoring data, or threatening to destroy data to extort money from companies.
- ATMs (Automated teller machines), EFT (Electronic funds transfer), EDI (Electronic data interchange), cellular phones are all vulnerable.
- Desktop publishing has made forgery and counterfeiting easier than it used to be, as isphone fraud.

Software theft

- Software theft costs the software industry an estimated $12 billion a year.
- Users have an opinion on the ethics of copying software that does not match the publishers and it is not always certain where the law stands on this around the world.
- Companies are not sure whether copyrights or patents is the best way to protect intellectual property and several look and feel cases have left the issues unresolved.
- The large question is how to protect intellectual property right without stifling creativity overall.
- **Filmy Hit, Tamil Rockers, Afilmywap** and other file-swapping sites have caused music and movies to be copied illegally and widely disseminated. It is estimated that such illegal product costs the music industry more than 500 crores of Rs. a year domestically (source: ITA web site).

Hacking

- Attacks by hackers and computer viruses have cost computer operators a great deal of time and money.
- Hackers have:
  - broken into computer systems to change exam results (and sometimes grades),
  - disrupted 100 systems,
  - hacked into Ministry computers
  - sold stolen data to the RAW and other Terrorist organizations
  - and blackmailed Innocent people and banks into hiring them as "security consultants."

Viruses

Viruses have erased file, damaged disks, and shut down computer systems. Below are some of the Infamous viruses in India

- **UHBVN Ransomware Attack**

Uttar Haryana BijliVitran Nigam was hit by a ransomware attack where the hackers gained access to the computer systems of the power company and stole the billing data of customers. **The attackers demanded Rs.1 crore or $10 million in return for giving back the data**.

- **WannaCry**

India was the third worst-hit nation by WannaCryransomware, **affecting more than 2 lakh computer systems**. During the first wave of attacks, this ransomware attack had hit banks in India including few enterprises in Tamil Nadu and Gujarat. The ransomware majorly affected the US healthcare system and a well-known French car manufacturing firm.

- **Mirai Botnet Malware Attack**

This botnet malware took over the internet, targeting home routers and IoT devices. This malware affected **2.5 million IoT devices including a large number of computer systems in India**. This self-propagating malware was capable of using exploitable unpatched vulnerabilities to access networks and systems.

- **Petya**

India was one of the top 10 countries to be hit by Petyaransomware. This ransomware attack halted work at one of the terminals of India's largest seaport causing computer lockdown and serious consequences for the country's exports.

- **BSNL Malware Attack**

The state-owned telecom operator BSNL was hit by a major malware attack, **impacting nearly 2000 broadband modems! 60,000 modems became dysfunctional after the malware attack** hit the Telecom Circle.

Netiquette

- "Netiquette" is network etiquette, the do's and don'ts of online communication. Netiquette covers both common courtesy online and the informal "rules of the road" of cyberspace.[1]
- When you enter any new culture - and cyberspace has its own culture - you're liable to commit a few social blunders. you might offend people without meaning to. Or you might misunderstand what others say and take offense when it's not intended. To make matters worse, something about cyberspace makes it easy to forget that you're interacting with real people - not just ASCII characters on a screen, but live human characters.
- There have been instances where "flame wars" (major verbal battles) have been place over the Internet because someone wrote something at which someone else took great offense - and the writer never intended it.

Privacy

- Safeguarding privacy in a modern society where so much information about us is public is extremely difficult if not impossible. There have been data disasters involving mistaken identities, data mix-ups, and doctored data which adversely affect people's lives, including driving and credit records.
- Aggravating the problem are the issues of calling number identification (CNID or Caller ID) monitoring of e-mail, and data marketing.

AI and Expert Systems

There is a hornets' net of issues associated by giving the computer the ability to make medical, legal, judicial, political and administrative decisions. Given what we know about unreliable software, is it wise to trust it? And what is product liability on this kind of matter.

Computers in the Workplace

This has led to 2 primary issues: repetitive stress syndrome (Carpal Tunnel disorder) and job monitoring, as well as other health-related issues.

Because of its constantly changing nature, the area of computer technology is one that is difficult to assign a specific set of moral codes, although it is necessary that ethics be considered when making decisions in this area. Computing creates a whole new set of ethical problems, unique unto itself.

Such problems include:

"…the unauthorized use of hardware, the theft of software, disputed rights to products, the use of computers to commit fraud, the phenomenon of hacking and data theft, sabotage in the form of viruses, responsibility for the reliability of output, making false claims for computers, and the degradation of work."

Ethical Dilemmas for Computer Users

- Some of these dilemmas are new (such as copying software), while others are new version of older problems dealing with right and wrong, honesty, loyalty, responsibility, confidentiality, trust, accountability, and fairness. Users face some of these problems while computer professionals face all of them.
- Some of these involve crimes, many that people frequently regard as "victimless" crimes. Are they truly victimless?
- Which is more important: access to affordable software or intellectual property rights? How do we protect developers so that they have the necessary incentive to be creative?
- Is hacking always wrong? Creating viruses?
- Who is responsible when a computer system fails to perform as it is supposed to? What kind of warranty should there be and from whom?
- What information on a database should be private? When are they doing us a service by providing that information?
- To what extent can we trust intelligent systems? Should we fund military systems?
- How should health hazards in the workplace be handled? Should we allow employers to monitor employee activities?

The Ten Commandments for Computer Ethics

1. You shall not use a computer to harm other people.
2. You shall not interfere with other people's computer work.
3. You shall not snoop around in other people's files.
4. You shall not use a computer to steal.
5. You shall not use a computer to bear false witness.
6. You shall not use or copy software for which you have not paid.
7. You shall not use other people's computer resources without authorization.
8. You shall not appropriate other people's intellectual output.
9. You shall think about the social consequences of the program you write.
10. You shall use a computer in ways that show consideration and respect.

Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:

Preamble:

1. **PUBLIC** - Software engineers shall act consistently with the public interest.
2. **CLIENT AND EMPLOYER** - Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.
3. **PRODUCT** - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.

4. **JUDGMENT** - Software engineers shall maintain integrity and independence in their professional judgment.
5. **MANAGEMENT** - Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
6. **PROFESSION** - Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
7. **COLLEAGUES** - Software engineers shall be fair to and supportive of their colleagues.
8. **SELF** - Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

Conclusion& Suggestions

As we continue to develop smart cities and smart grid technologies in 2021, the risk of ransomware attacks will stay put as a big challenge for all organizations. Apart from focusing on development and advancement, every industry vertical must understand the crucial role of cyber security.

With the help of these below listed proactive measures organizations can reduce or prevent the constantly evolving ransomware attacks in the future:

Employee Awareness Training

Cyber threat actors majorly use emails as bait in attempting cyber-attacks on an organization and humans being the weakest link tend to easily fall for it. So to avoid and overcome this problem, organizations must educate their employees by making them aware of the prevailing cyber threats.

A right security attack simulator and awareness training tool can help in reducing the threat of employee error. Such tools help in mitigating existing cyber risks within the organization and enhance the cyber security posture.

Backup Your Data Separately

The best way to stay proactive is by backing up your data in a separate external storage device but it should not be connected to your computer. Backing up your data will help in securing it from being encrypted and misused by cyber attackers.

Regular Vulnerability Assessment

Basic cyber security hygiene like vulnerability assessment and penetration testing can help in preventing malware like ransomware. With the help of continuous vulnerability assessment, one can find out the exploitable vulnerabilities and fix them before any threat actor discovers it.

Never Click on Unverified Links

Avoid clicking links that are attached in spam emails or on an unfamiliar website. Such links are the bearers of malicious files that badly infect the user's computer when clicked. Moreover, these links are the pathways for ransomware to access the user's system and encrypt or lock confidential data for ransom.

II. REFERENCES

[1]. https://kratikal.com/blog/the-6-biggest-ransomware-attacks-that-happened-in-india/
[2]. 1http://albion.com/netiquette
[3]. https://www.meity.gov.in/
[4]. https://www.childlineindia.org/a/issues/online-safety?gclid=EAIaIQobChMIsfKoztLL_QIVKZlmAh3jnAqOEAAYAiAAEgLyJPD_BwE
[5]. https://www.aicte-india.org/CyberSecurity