**The problem you are analyzing:** "Cyber Security: Threats and challenges."

**Statement of the problem:**

The growing digital era of computers and smart devices has provided many opportunities, from sharing personal information to express our opinions digitally but, how often do we think before leaving those digital footprints? According to the 12th Global Risk Report published by the World Economic Forum (WEF), cybersecurity threats are among the top 10 risks in modern society. When we think about cybersecurity, we restrict our minds only to personal information, whereas in reality, the term cybersecurity cannot restrict to the personal or organizational level. The problem we are analyzing deals with how cybersecurity impact our digital world and what are the various threats and challenges involved in cybersecurity.

**The key question at issue is:**

There have been rising demands of smart devices with high computational power backed with the capability of storing and processing vast amounts of data. The critical question here is to understand if these devices are capable enough to store the data securely and ethically? Also, how can it be ensured that the stored data does not make the user feel vulnerable? Is there a necessity to create awareness of how the threats on data have increased way beyond just the theft of the device storing and generating them? What are the economic and social problems arising from such security challenges? And lastly, are there enough legislations to curb the menace of cyber-attacks and cybercrime?

**Purpose of reasoning through the issue is:**

The purpose of making cyberspace safe and secure is manifolds. The first reason is that smartphones combined with the power of convenient storage like clouds have led users in storing sensitive personal information ranging from bank details to photos/ videos on large scales. Creating a safer environment for storing such crucial information can ensure the users' right to privacy not being violated. Second, smartphones, as well as a range of other smart devices, are predicted to be monitoring and recording the data generation patterns of the user. This data collected is used to create targeted marketing for other companies. The third reason is that users in most of the cases are not aware of the sensitive data being generated and used without their consent. Ensuring that there are enough laws placed can help users to exercise their rights to privacy. Lastly, the connectivity of devices to the outside world via the internet has also become a liability issue and has made the user highly prone to intrusion attacks. Threats are ranging from leaking of data when connected to unsecured Wi-Fi to spoofing or phishing attacks caused by small bugs stored inside the webpages. Other threats involve using applications from untrusted sources have opened more gates than ever before for unauthorized users to access data quickly. Finally, the impact of cybercrime on financial health and social issues cannot be ignored. Therefore, there exists an urgent need to spread awareness regarding cybersecurity threats and challenges.

**Information**

With the advent of afloat news about significant data leaks from products related to technological giants like Apple, Facebook etc. have created chaos within the user community. Hence significant research from credible sources must be used to build case studies to test the various attacks possible on the data stored on the personal devices. Once triggered, the attackers could readily get excess to personal data of hundreds to thousands of people within a few minutes without any information of the incident to the user. Further, these case studies must be used to create higher security of the devices. Information on the types of attacks and different ways to protect the data from these attacks must also be provided to the users to increase the overall security. Awareness must be spread about the necessity of personal verification of terms and conditions of the products before it is accepted.

**Assumptions:**

The common assumption made in the cybersecurity domain is that the communicating channel and pre-existing network protocols are sufficient enough to protect the data transmitted. Assumptions made that only the existing types of attack can occur. Attacks on the devices targeted; hence a bland assumption is made that devices like mobile phones, laptops owned by the general public are safe from any form of cyber-attacks. The user generally assumes that the security of the data is rarely their responsibility, and there is nothing that can be done on their end to secure it. An assumption made about the usage and data storage capabilities of the smart device. An assumption made that the user has no right and has to accept the terms and conditions of the product/ software to use it.

**Concepts(final check is done):**

The term cybersecurity not only involves the protection of data, communication channel and network around us, but it covers a wide and crucial area in the cyber world. The concept of cybersecurity becomes even more critical when smart devices are taken into consideration.

Cybersecurity threats can broadly be divided into three parts. First, Cyberterror which involves activities leading to terrorism using cyberspace. Second, cybercrime, the primary goal is to extract confidential information through unethical methods. Lastly, Cyberwar which involves hampering others nation cyberspace and network using different intrusion attacks such as DDoS attack or man in the middle attack.

**Implication:**

The data stored without the highest levels of security might lead to severe implications such as Identity Thefts where the attacker takes benefits from services pretending to be someone he is not, Financial Threats wherein the leak of bank data or credit card numbers etc. might lead to unauthorized transactions. Other common issues that arise due to lack of security of the data in the cyber environment are the sharing of unethical photos and videos with intentions to disgrace people etc. On the more severe level lack of cybersecurity also leads to security threats like cyber warfare and cyber terror were nations might use data to attack other nations causing significant harm.

**Point of view:**

From the IT industry professionals analyzing the future, the current scenario of booming data production predicts much higher generation rates. The protection of data from cyber and malicious attacks is of utmost importance. A single attack and theft of information can harm millions of users in a single blow. A small vulnerability can risk the information leak of many. IT industry loses millions of dollars in case their data gets breached as in the examples of Target and Sony in the past. The perspective of whistleblowers like Edward Snowden and WikiLeaks, which leaked classified data about the National Security, which aimed to disclose the government's unethical means of generation and usage of sensitive data. On the other hand, the perspective of government agencies is that the data collected and analyzed from various sources are to be used for national security purposes and the protection of their citizens.

**Inference / conclusion**

After understanding the issues and point of view, it is imperative to protect these devices from cyber threats. It is equally important to educate and spread awareness amongst people who are not directly linked to the IT sector and know little about the risks of cybersecurity threats. The IT companies should invest equally in the development as well as the security of their products. It is the responsibility of the organization storing data to safeguard it from cyber-attacks. More resources are needed to develop cybersecurity programs across the globe as they are needed today as never before.

**Summary:**

After critically and logically analyzing the severe threats the cyber domain is facing today, a conclusion can be drawn that the significant portion of menace occurs because of the negligence of the user. This negligence occurs as the users are mostly undereducated and misinformed about the vulnerabilities their data holds. The users have to be informed about how the digital exhaust left by them leaves them at higher risks of cybercrimes. On the technical level professionals have to be cautious about whom they share sensitive information with, and the best level of security affordable by the companies must be implemented. This analysis can further be summarized by the words of the great American cryptographer Bruce Schneier "If you think technology can solve your security problems, then you don't understand the problems, and you don't understand the technology."