



# CYBER SECURITY: AN OUTLINE OF ITS TYPES, ELEMENTS AND VENDORS

Rahul Kumar Varma

Institute of Distance and Open Learning, University of Mumbai

## ABSTRACT:

Cyber security is the state or process of protecting and recovering networks, devices, and programs from any type of cyber-attack. Cyber-attacks are an evolving danger to organizations, employees, and consumers. They may be designed to access or destroy sensitive data or extort money. They can, in effect, destroy businesses and damage people's financial and personal lives. This paper discusses the types and elements of cyber security. It also proposes the benefits of cyber security listing the vendors of cyber security field.

## KEYWORDS:

Cyber Security, Cyber Attacks.

## INTRODUCTION:

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.

Cyber Security is vital as government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber-attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. Cyber-attacks and digital spying are the top threat to national security, eclipsing even terrorism.

## OBJECTIVE:

1. To understand the concept of Cyber Security.
2. To know the types of Cyber Security.
3. To learn the elements and benefits of Cyber Security.
4. To know the Vendors in Cyber Security field.

## Types of Cyber Security:

- **Ransomware:** Ransomware is a type of malware that involves an attacker locking the victim's computer system files through encryption and demanding a payment to decrypt and unlock them.
- **Malware:** Malware is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.
- **Social Engineering:** Social Engineering is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.
- **Phishing:** Phishing is a form of fraud where fraudulent emails are sent that resemble emails from reputable sources; however, the intention of these emails is to steal sensitive data, such as credit card information or login information (Use Id and Password).

**Cyber Security Elements:** Ensuring cyber security requires the coordination of efforts throughout an information system, which includes:

- Application Security
- Information Security
- Network Security
- Disaster Recovery / Business Continuity Planning
- Operational Security
- End-User Education.

## Cyber Security Benefits:

- Business protection against malware, ransomware, phishing and social engineering.
- Protection for data and networks.
- Prevention of unauthorized users.
- Improves recovery time after a breach.
- Protection for end-users.
- Improved confidence in the product for both developers and customers.

**Cyber Security Vendors:** Vendors in cyber security fields will typically use endpoint, network and advanced threat protection security as well as data loss prevention. Three commonly known cyber security vendors include Cisco, McAfee and Trend Micro.

- **Cisco:** Cisco tends to focus on networks and allows its customers to utilize firewalls, VPNs and advanced malware protection along with supporting email and endpoint security. Cisco also supports real-time malware blocking.
- **McAfee:** McAfee makes cyber security products for consumers and enterprise users. McAfee supports mobile, enterprise clouds, network, web and server-based security. Data protection and encryption is also offered.

- **Trend Micro:** Trend Micro is an anti-malware vendor which offers threat protection for mobile, hybrid clouds, SaaS and the IoT. Trend Micro provides users with endpoint, email and web security.

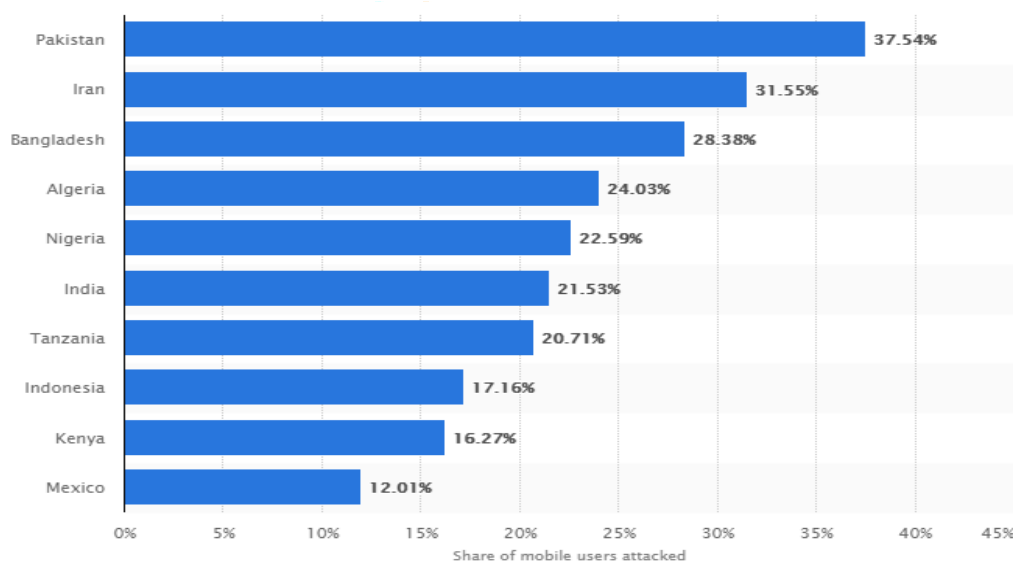
## METHODOLOGY:

Primary data was not collected for the research paper.

### Secondary Data

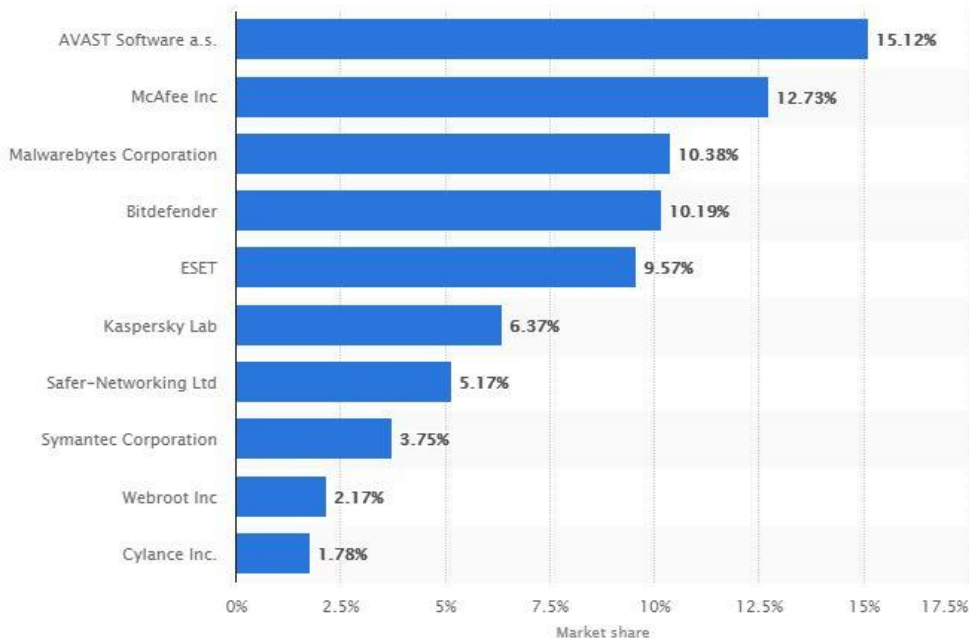
The secondary data has been collected. For this purpose various magazines and journals have been used as it is a conceptual paper. Thus, the focus is to know more about the concept, its application and the impact on economy via other parameters. Therefore qualitative and quantitative data have been used.

### Percentage of mobile users who have fallen victim to mobile malware infections in 1st quarter 2019, by country



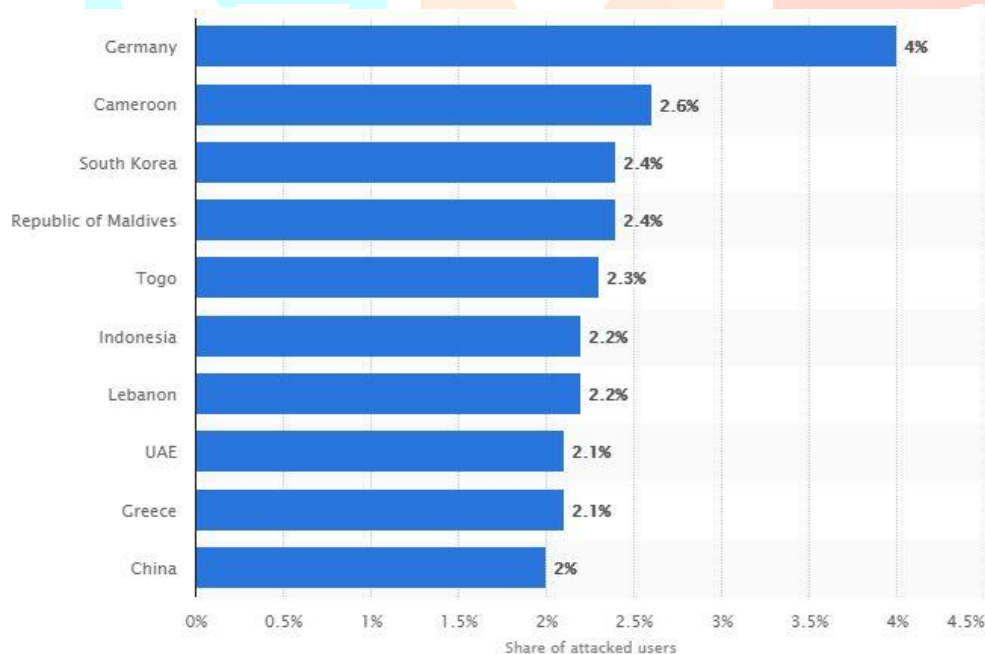
The above statistic shows the top ten countries attacked by malicious mobile malware in the first quarter of 2019. More than a third of all mobile users in Pakistan were attacked by mobile malware during the measured period.

Market share held by the leading Widows anti- malware application vendors worldwide, as of January 2019



This statistic shows the market share held by anti-malware vendors that offer applications designed for Windows as of January 2019. At that time, Avast held 15.12 percent of the anti-malware application market. China, Taiwan and Turkey are the countries with the highest rate of malware-infected computers. Sweden, Norway, and Japan are among the countries with the lowest rates of malware infection.

Countries most targeted by banking malware attacks from Nov 2017 to Oct 2018



This statistic shows a ranking of the countries most targeted by banking malware attacks from November 2017 to October 2018. During the measured period, four percent of users in Germany were attacked by banking malware.

**CONCLUSION:**

Cyber security is essential for small, midsize and large organizations in order to detect computer usage and prevent any illegal activities are conducted on the computer systems. A cyber security survey can be conducted to understand the various types of computers being used by customers, avoid hacking on any of the existing computer systems, which antivirus is being currently used and other such angles related to cyber security.

**REFERENCES:**

1. <https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html>
2. <https://iopscience.iop.org/article/10.1088/1757-899X/263/4/042043>.
3. <https://digitalguardian.com/blog/what-cyber-security>.
4. <https://economictimes.indiatimes.com/definition/cyber-security>.
5. <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>
6. <https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security>
7. <https://currentaffairs.adda247.com/india-3rd-most-vulnerable-country-to/>
8. <https://www.questionpro.com/blog/computer-security-survey-questions/>
9. <https://www.statista.com>

