Introduction to Internet Security

What is Internet Security?

- *is a catch-all term for a very broad issue covering security for transactions made over the Internet. Generally, Internet security encompasses browser security, the security of data entered through a Web form, and overall authentication and protection of data sent via Internet Protocol.*
- *Internet security is a branch of computer security which comprises various security measures exercised for ensuring the security of transactions done online. In the process, the internet security prevents attacks targeted at browsers, network, operating systems, and other applications. Today, businesses and governments are more concerned about safeguarding from Cyber attacks and malware programs that originate from the internet. The main aim of Internet security is to set up precise rules and regulations that can deflect attacks that arise from the Internet.*
- *Internet security relies on specific resources and standards for protecting data that gets sent through the Internet. This includes various kinds of encryption such as Pretty Good Privacy (PGP)*
- *Internet security is generally becoming a top priority for both businesses and governments.*

What is Cybersecurity?

- *is the protection of internet-connected systems, including hardware, software and data, from cyber-attacks. In a computing context, security comprises cybersecurity and physical security -- both are used by enterprises to protect against unauthorized access to data centers and other computerized systems*

- *Cyber security is important because 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.*

CHALLENGES OF CYBER SECURITY

For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system. Elements of cyber encompass all of the following:

- ***Network security:*** *The process of protecting the network from unwanted users, attacks and intrusions.*
- ***Application security:*** *Apps require constant updates and testing to ensure these programs are secure from attacks.*
- ***Endpoint security:*** *Remote access is a necessary part of business, but can also be a weak point for data. Endpoint security is the process of protecting remote access to a company's network.*
- ***Data security:*** *Inside of networks and applications is data. Protecting company and customer information is a separate layer of security.*
- ***Identity management:*** *Essentially, this is a process of understanding the access every individual has in an organization.*

- ***Database and infrastructure security:*** *Everything in a network involves databases and physical equipment. Protecting these devices is equally important.*
- ***Cloud security:*** *Many files are in digital environments or "the cloud". Protecting data in a 100% online environment presents a large amount of challenges.*
- ***Mobile security:*** *Cell phones and tablets involve virtually every type of security challenge in and of themselves.*
- ***Disaster recovery/business continuity planning:*** *In the event of a breach, natural disaster or other event data must be protected and business must go on. For this, you'll need a plan. End-user education: Users may be employees accessing the network or customers logging on to a company app. Educating good habits (password changes, 2-factor authentication, etc.) is an important part of cybersecurity.*

The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves. Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known treats. Today, this approach is insufficient, as the threats advance and change more quickly than organizations can keep up with. As a result, advisory organizations promote more proactive and adaptive approaches to cyber security. Similarly, the National Institute of Standards and Technology (NIST) issued guidelines in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessments, a data-focused approach to security as opposed to the traditional perimeter-based model.

Israel is one of the leading countries specializes in cybersecurity.