What is Cyber-Security?

Cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- **Information security** protects the integrity and privacy of data, both in storage and in transit.
- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or

data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

- **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

The scale of the cyber threat

The U.S. government spends $19 billion per year on cyber-security but warns that cyber-attacks continue to evolve at a rapid pace. To combat the proliferation of malicious code and aid in early detection, the National Institute of Standards and Technology (NIST) recommends continuous, real-time monitoring of all electronic resources.

The threats countered by cyber-security are three-fold:

1. Cybercrime includes single actors or groups targeting systems for financial gain or to cause disruption.

2. Cyber attack often involves politically motivated information gathering.

3. Cyberterror is intended to undermine electronic systems to cause panic or fear.

Common methods attackers use to control computers or networks include viruses, worms, spyware, Trojans, and ransomware. Viruses and worms can self-replicate and damage files or systems, while spyware and Trojans are often used for surreptitious data collection. Ransomware waits for an opportunity to encrypt all the user’s information and demands payment to return access to the user. Malicious code often spreads via an unsolicited email attachment or a legitimate-looking download that actually carries a malware payload.

Cyber-security threats affect all industries, regardless of size. The industries that reported the most cyberattacks in recent years are healthcare, manufacturing, finance, and government. Some of these sectors are more appealing to cybercriminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks.

End user protection

So, how do cyber-security measures protect users and systems? First, cyber-security relies on cryptographic protocols to encrypt emails, files, and other critical data. This not only protects information in transit, but also guards against loss or theft. In addition, end-user security software scans computers for pieces of malicious code, quarantines this code, and then removes it from the machine. Security programs can even detect and remove malicious code hidden in Master Boot Record (MBR) and designed to encrypt or wipe data from computer's hard drive.

Electronic security protocols also focus on real-time malware detection. Many use heuristic and behavioral analysis to monitor the behavior of a program and its code to defend against viruses or Trojans that change their shape with each execution (polymorphic and metamorphic malware). Security programs can confine potentially malicious programs to a virtual bubble separate from a user's network to analyze their behavior and learn how to better detect new infections.

Security programs continue to evolve new defenses as cyber-security professionals identify new threats and new ways to combat them.

Cybersecurity Defined

Also referred to as information security, cybersecurity refers to the practice of ensuring the integrity, confidentiality, and availability (ICA) of information. Cybersecurity is comprised of an evolving set of tools, risk management approaches, technologies, training, and best practices designed to protect networks, devices, programs, and data from attacks or unauthorized access.

Why is Cybersecurity Important?

The world relies on technology more than ever before. As a result, digital data creation has surged. Today, businesses and governments store a great deal of that data on computers and transmit it across networks to other computers. Devices and their underlying systems have vulnerabilities that, when exploited, undermine the health and objectives of an organization.

A data breach can have a range of devastating consequences for any business. It can unravel a company's reputation through the loss of consumer and partner trust. The loss of critical data, such as source files or intellectual property, can cost a company its competitive advantage. Going further, a data breach can impact corporate revenues due to non-compliance with data protection regulations. It's estimated that, on average, a data breach costs an affected organization $3.6 million. With high-profile data breaches making media headlines, it's essential that organizations adopt and implement a strong cybersecurity approach.

Common Types of Cybersecurity

Network Security protects network traffic by controlling incoming and outgoing connections to prevent threats from entering or spreading on the network.

Data Loss Prevention (DLP) protects data by focusing on the location, classification and monitoring of information at rest, in use and in motion.

Cloud Security provides protection for data used in cloud-based services and applications.

Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) work to identify potentially hostile cyber activity.

Identity and Access Management (IAM) use authentication services to limit and track employee access to protect internal systems from malicious entities.

Encryption is the process of encoding data to render it unintelligible, and is often used during data transfer to prevent theft in transit.

Antivirus/anti-malware solutions scan computer systems for known threats. Modern solutions are even able to detect previously unknown threats based on their behavior.