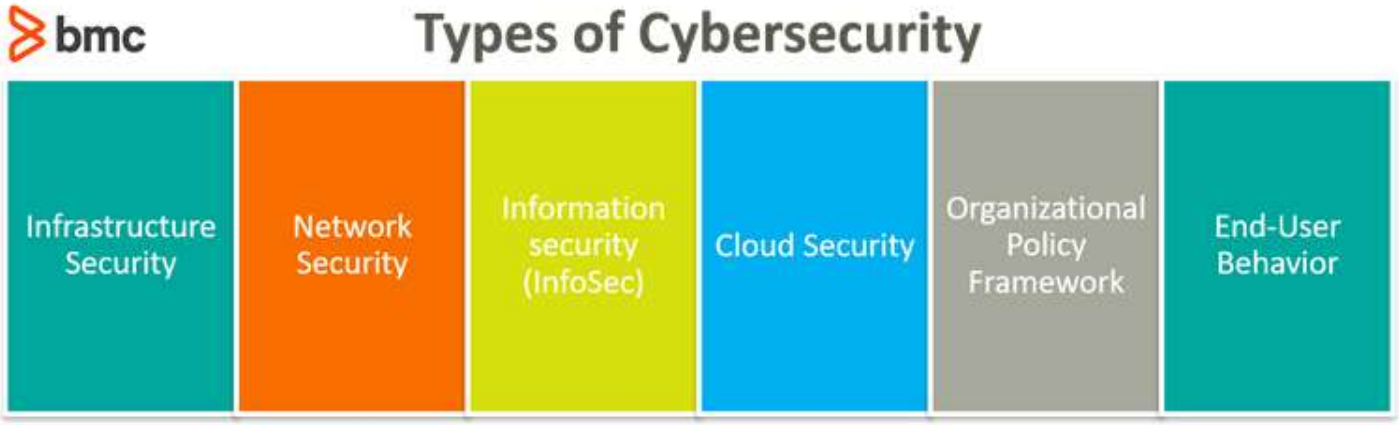
Types of cybersecurity

Cybersecurity can be applied to a variety of categories across the technology stack, from user-facing applications and backend network infrastructure to organizational policies and end-user behavioral practices. Here are the most common categories of cybersecurity:



Infrastructure Security

Relates to the security of utility services infrastructure use to power and operate datacenter technologies, cloud, and networks. A cyber-attack causing power outages at datacenters are often aimed at its critical utility infrastructure systems. Examples of this infrastructure include:

- Power supply and transmission systems
- Water supply and cooling
- Heating and ventilation
- Other cyber-physical systems

Network Security

Data must be secured during transmission. Network security measures such as encryption, traffic monitoring, firewalls, Virtual Private Networks (VPNs), and end-point security ensure data integrity as it transmits between servers and clients across distributed networks.

Information Security (InfoSec)

Involved with the security of data across its end-to-end lifecycle, InfoSec measures are designed to ensure that only the authorized users, apps, and systems are able to access the required information. The main objectives of information security include confidentiality, integrity and availability (CIA) of data. Additional objectives include accountability and authenticity of information, which contribute to the overall security and privacy associated with digital information.

Cloud Security

Digital information, apps, and services typically reside in servers across geographically distributed data centers accessed over Internet networks. These data centers, known as cloud systems, should be secure and designed to meet Service Level Agreement (SLA) objectives as decided between cloud vendors and its customers. Cloud security ensures that this infrastructure and the data stored in cloud systems is secure against cyber threats. Other objectives include that privacy and service availability is ensured within a network of shared cloud infrastructure resources.

Organizational Policy Framework

Your organizational policy framework is the part of cybersecurity responsible for mitigating security risks. It relates to everything, ranging from the choice of cybersecurity solutions, access controls and privileges assigned to end-users, disaster response, and preparation. The policy framework should be designed as an optimal tradeoff between security, cost, performance and business value of cybersecurity initiatives.

End-User Behavior

Users are the first line of defense against cyber-attacks. Many security vulnerabilities in technologies and systems can be addressed by controlling the human element compromised with a cyber-attack. Educating users about the security best-practices such as regularly updating systems for security, keeping strong passwords and authentication systems, and not exposing critical corporate information and digital workloads to security-prone IT environments and situations is the first step for any cybersecurity program.