NETWORK SECURITY

By: **Dream Tech LLC**

NETWORK SECURITY

- 1 aspect of cyber defense-in-depth that focuses on deploying security controls and processes involving both hardware/software to protect information from intrusions and threats.
- Involves People, processes and policies related to rules, configurations, accessibility for overall threat protection and relief.

WHY IS IT IMPORTANT?

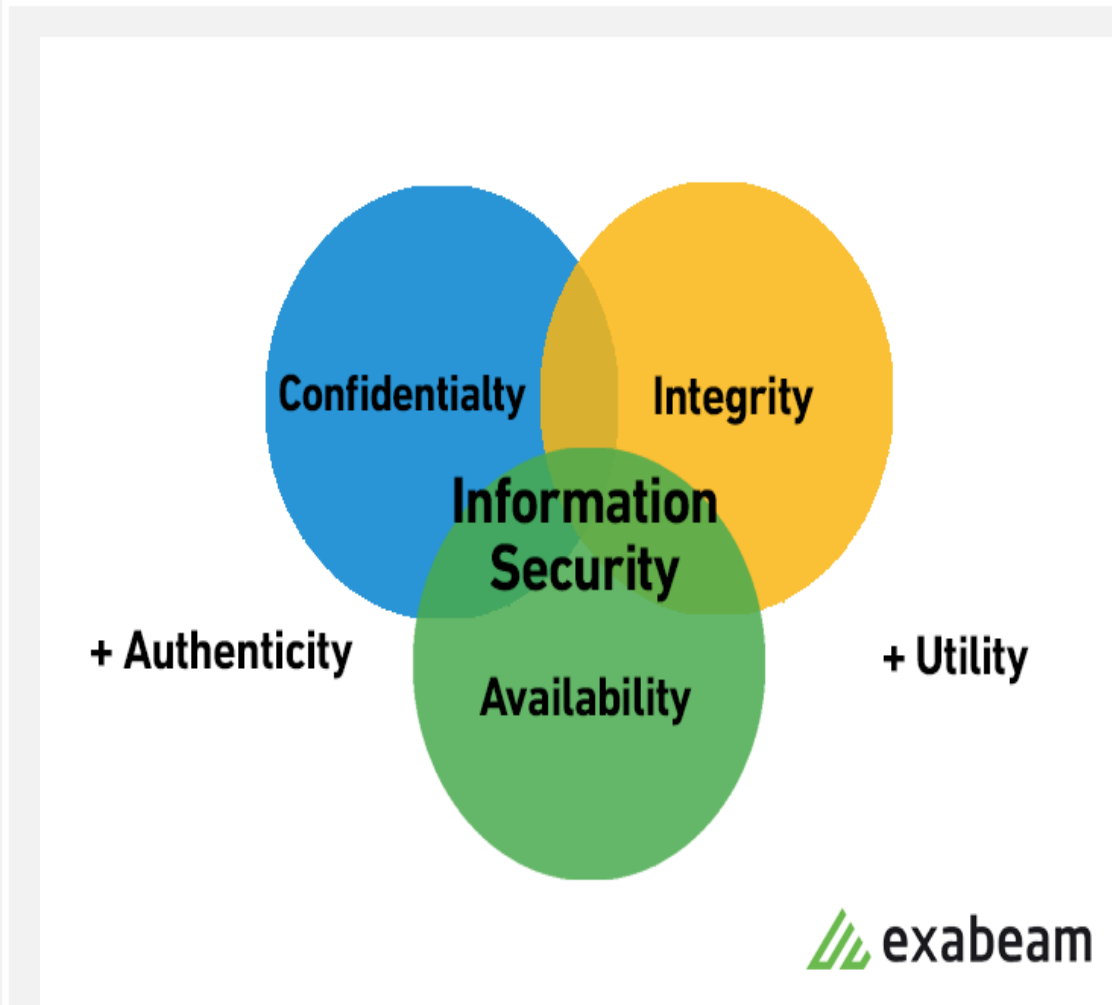
1) Requirement
2) Data breaches costs more money to respond to
3) Cyber-attacks are constantly rising and have become APT's
4) Prevents data loss
5) Promotes business continuity
6) Fines and legal ramifications
7) Loss of business

TYPES OF NETWORK SECURITY PROTECTIONS

- Access control
- Anti –malware
- Application security
- Firewalls
- VPN encryption
- IDS/IPS
- DLP
- Segmentation

BENEFITS OF NETWORK SECURITY

- Reducing overhead of breach recovery expenses (investment v.s. response)
- Safeguards sensitive information (Client & employee)
- Streamline business processes
- Successful delivery of products and services
- Ensure legitimate access to systems, applications and data for safe and secure delivery of products and services to customers
- Ensure reliability & [performance of network functionality



3 KEY FOCUSES

- **Protection**

- Involves the security tools and policies deployed to prevent malicious network intrusions and disruptions

- **Detection**

- The resources necessary to allow the analysis of network traffic in real-tie and identify any deviations of normality before they evolve and transform to cause impact and long-term harm to information

- **Response**

- The ability to react and triage to discovered security threats and resolve them as quickly as possible and prevent further concern with deploying technical and administrative security controls

TOOLS/TECHNIQUES

- Access control
- Anti-threat software/hardware appliances
- Anomaly detection such as IDS/IPS systems
- Application Security
- (DLP) Data loss prevention
- Email Security
- (EDR) Endpoint detection & response
- Firewalls
- Network segmentation
- (SIEM) Security information and event management
- (VPN) Virtual private network
- Web security

BEST PRACTICES

- Network audit

- Assess vulnerabilities, unused ports/applications, and backups

- Deployment of security devices (Monitor, detect & triage)

- WAF ,IDS/IPS and SIEM

- Patch management; Periodic system and device pushed updates

- Disable file sharing features

- Address all 3 layers; Technical, Physical and Administrative

- Operate critical servers within a (DMZ) Demilitarized zone

- Conduct annual or bi-annual penetration tests on all critical systems