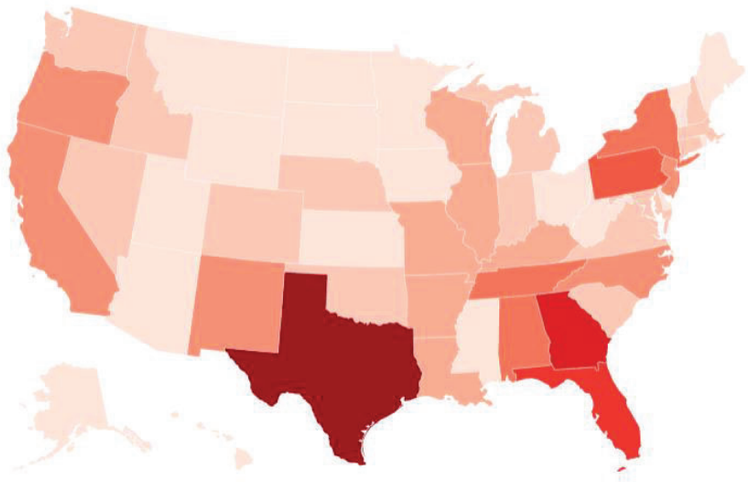

PEAR TREE SERVICES
Business Technology Solutions
CYBER SECURITY RISK ASSESSMENTS
THE ULTIMATE GUIDE

Organizational CyberSecurity Responsibilities for 2021

Cybersecurity is not solely an IT responsibility but an Organizational objective. Cybersecurity 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. 75% to 85% of threats come from internal within customers Network. The term Cybersecurity 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 cybersecurity 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.

Ransomware attacks cost local and state governments over $18 billion in 2020



In 2020, Texas had the highest number of attacks and the greatest number of people impacted (58.3 million). The reason for such a high number of people being affected is that two statewide departments were attacked – the Texas Court of Administration and the Texas Department of Transportation. This potentially impacted each Texan twice.

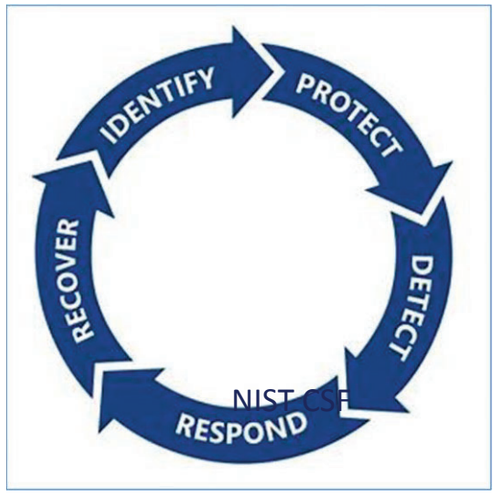
Source: American City and County – March 22, 2021

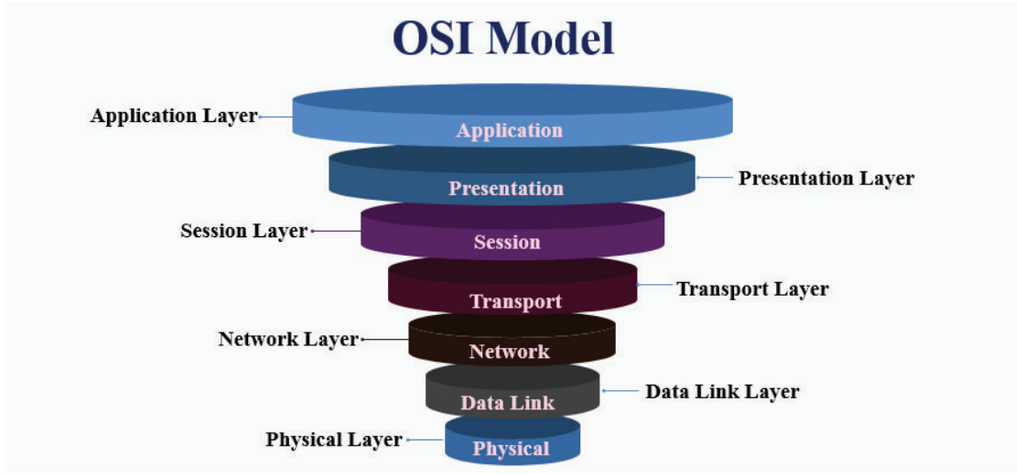
PEAR TREE SERVICES
Business Technology Solutions

- Onsite / Remote Risk Assessments
- Cybersecurity Training
- Phishing Campaigns
- USB Drop Campaigns
- Network Vulnerability Scanning
- Network Security Architecture Planning
- Compliance Adherence (HIPAA, PCI DSS, CJIS, etc.)

PEAR TREE SERVICES
Business Technology Solutions

PEAR TREE Technology Solutions Cybersecurity Offerings are built using the NIST CSF, and the Open Systems Interconnection (OSI) Security Layers.





PEAR TREE SERVICES
Business Technology Solutions

Cybersecurity Risk Assessment

NIST Cybersecurity Framework

Identify, Protect, Detect, Respond, Recover

Identify	Protect	Detect	Respond	Recover
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology	• Anomalies and Events • Security Continuous Monitoring • Detection Processes	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Recovery Planning • Improvements • Communications

Physical Security

Environmental Controls

Server / Workstation Security

Vulnerability Scans

Penetration Testing Scans

Dark Web Scanning

Assessment Report

Remediation Plan

PEAR TREE SERVICES

Business Technology Solutions

Next Steps?

- Determine the security vulnerabilities of your existing network
  - Recommend an independent IT Health & Security Assessment
  - Assessments should review all elements of infrastructure:
    - ✓ Server hardware age, warranties, and operating system
    - ✓ Desktop hardware age, specifications and operating system
    - ✓ Network switch hardware age, specifications and connections
    - ✓ Network Firewall age, warranty, connections & configurations
    - ✓ Antivirus & Patching status
    - ✓ Data Backup, Security & Recoverability

PEAR TREE SERVICES
Business Technology Solutions


CYBER SECURITY
PRIVACY
PROTECTION
COMPUTER
DEVICES
SYSTEM
NETWORK
ACCESS
PEAR TREE SERVICES
Business Technology Solutions