Orange County Transportation Authority
Cyber Security Update

Regulations and Policy

The OCTA Cyber Security Program is built to comply with or address:

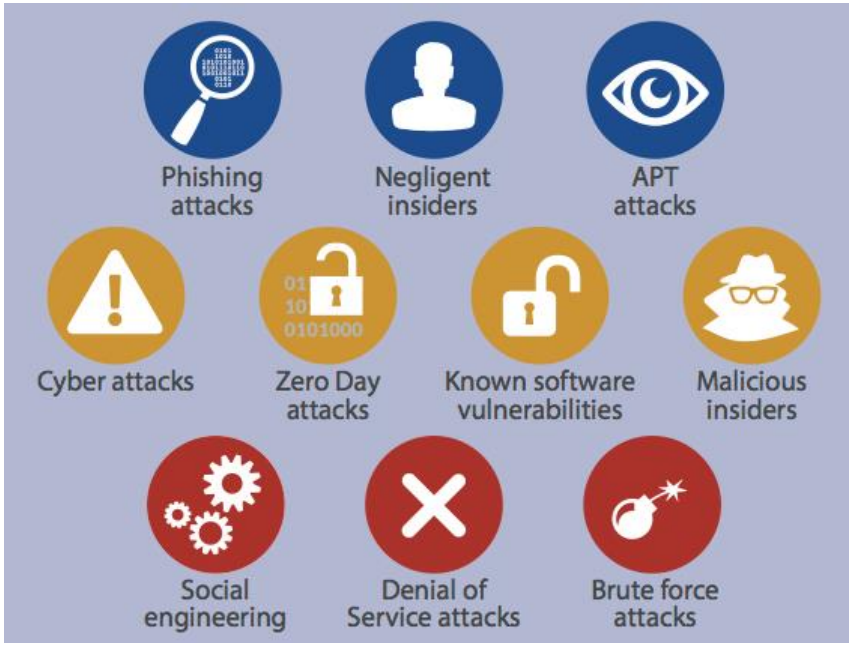
- Federal Act Guidance and Best Practices
- California Requirements
- External Organizational Standards
- OCTA Mission, Business Impact Analysis, Continuity of Operations Plan, and Policies

Understanding Current Threats

Cyber vulnerabilities are constantly evolving.

A successful security program takes into account current industry trends and defines priorities based on threats, not just vulnerabilities.

- California had nearly double the victims of cyber crime than the next closest state, with phishing as the top reported crime (FBI IC3 report)
- Enterprise Ransomware was up 12 percent in 2019. (Symantic)
- Average cost of a breach in US is $8.19 million (IBM)



OCTA Cyber Security Posture

OCTA follows industry best practices and continually builds on:

- Administrative plans, policies, and procedures
- Next generation security tools and services
- 3rd party cybersecurity support for monitoring and incident response
- Automated and in-person security training
- Independent assessments and audits
    - Microsoft, Palo Alto, Secureworks, National Cyber security Review, Gartner, and External and Internal Auditors.

Security Projects and Accomplishments

- ✓Next Gen firewalls and services
- ✓Enhanced phishing testing/training
- ✓Enhanced patching and remediation
- ✓O365 conditional access controls
- ✓Workstation upgrades & hardening
- ✓Server upgrades & hardening
- ✓Change management automation
- ✓Payment Card Industry compliance improvements
- ✓Continued network segmentation
- ✓Increased network monitoring
- ✓Strengthened vulnerability remediation program
- ✓Strengthened incident response program and capabilities
- ✓Strengthened cyber security policies

Cyber Security Roadmap

As OCTA continues to provide our customers with new and more efficient ways to access our services, cyber security has had to evolve.