



TOP TEN

IT & CYBERSECURITY INITIATIVES FOR FINANCIAL SERVICES

IT & CYBERSECURITY INITIATIVES FOR FINANCIAL SERVICES

1. AGGRESSIVE IDENTITY MANAGEMENT.

A robust onboarding and offboarding process combined with choosing an identity provider for Single Sign On (Single Shut Off) functionality. Leverage SSO to enhance security around the #1 attack surface, user identity.

2. ENDPOINT MANAGEMENT.

Workstations and mobile devices are, now more than ever, the entry point to systems and data. Endpoints must be controlled to reduce the likelihood of compromise. Use mobile device management and conditional access policies to shrink the vast attack surface that is SaaS applications.

3. AGGRESSIVE VULNERABILITY PATCHING.

Turning on automatic updates is NOT enough. New vulnerabilities are disclosed daily, and you need a robust process and mechanism to patch critical vulnerabilities.

4. MONITORED NEXT-GENERATION ANTIVIRUS AND ENDPOINT DETECTION & RESPONSE (AV & EDR) SOFTWARE.

It isn't enough to install AV and EDR. You need a qualified team monitoring and proactively responding to telemetry from AV & EDR.

5. SECURE REMOTE ACCESS.

The remote workforce is particularly vulnerable to network layer attacks. Traditional VPN connections and VPN services are no longer adequate. Employ Secure Access Service Edge (SASE) services to monitor, block, and alert on network born threats. Reduce the attack surface by tunneling traffic through known/trusted gateways.

6. ROUTINELY ASSESS YOUR SECURITY POSTURE.

Consult professionals to routinely assess your security posture relative to the quickly changing threat landscape. While difficult at first, risk assessment can and should become a cultural norm.

7. TEST YOUR DEFENSES.

Utilize social engineering, vulnerability scanning, and penetration testing to see if your policies and controls meet your objectives. Consider ongoing social engineering testing services to strengthen your weakest link, people.

8. ENCRYPT YOUR DATA.

Make sure all confidential, sensitive, and PII data is encrypted at rest and in transit. Encrypt servers, endpoints (mobile devices & workstations) and be sure all data transfer methods are encrypted. API keys need to be secured, and procedures put in place to rotate any keys that are vulnerable or compromised.

9. EXCELLENT PASSWORD HYGIENE.

Use long, strong, complex and unique passwords, period. Passwords should ONLY be stored in a secure, encrypted password vault. Do NOT store passwords in browsers. Use an enterprise password manager to help the organization monitor password hygiene (without divulging credentials) and improve over time.

10. CYBERSECURITY FRAMEWORK

Consider adopting a cybersecurity framework to aid your organization in considering, addressing, and monitoring the most common risks.