



### REPORT CARD:

## GREATER HOUSTON AREA

# ACCOUNTING FIRM DOMAIN CYBERSECURITY

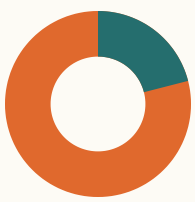
CinchOps assessed over 730 accounting firm domains across Greater Houston, evaluating six critical security categories. Only 32% of firms achieved acceptable security standards, highlighting significant vulnerabilities in Houston's accounting sector.

#### Security Scan Summary for Domain Security

### Domain Security Pass/Fail

Passing Grades are A+B, Failing Grades are C+D

■ Pass ■ Fail



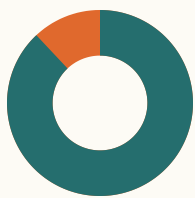
Application Security  
21% / 79%



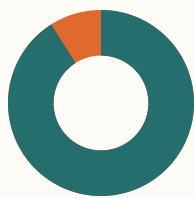
DNS Health  
45% / 55%



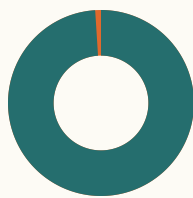
Network Security  
32% / 68%



IP Reputation  
88% / 12%



External Vulnerabilities  
91% / 9%

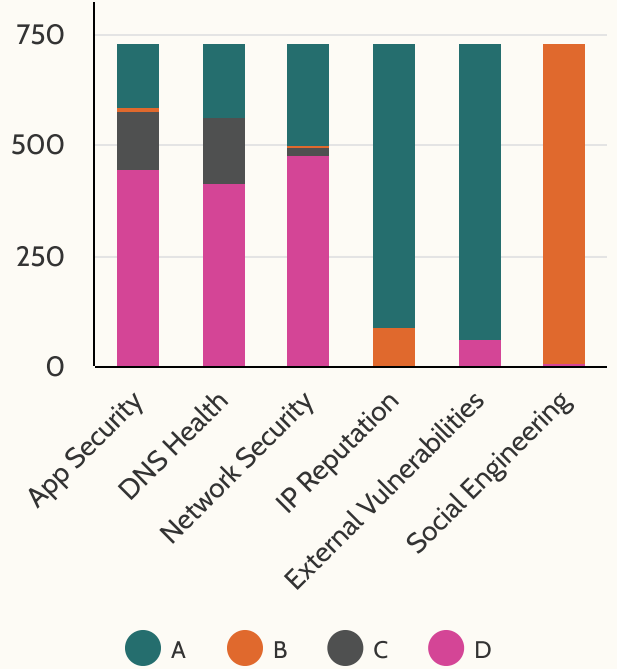


Social Engineering  
99% / 1%

The comprehensive security assessment reveals critical exposures among Greater Houston accounting firms. Most firms demonstrated severe weaknesses in application security, DNS health, and network infrastructure, creating entry points for cybercriminals targeting sensitive financial data.

While firms showed stronger performance in reputation management, the overall assessment indicates that the vast majority operate with insufficient security postures against common cyber attacks targeting financial service providers.

### Security Audit Grade Distribution



### Progress Report

Accounting firms demonstrated a stark divide in cybersecurity performance across security domains. The most concerning results appeared in application security, DNS health, and network security, where firms consistently earned failing grades, indicating widespread vulnerabilities in foundational digital infrastructure.

Social engineering resilience showed moderate performance, while firms achieved good grades in external vulnerability management and IP reputation maintenance. Despite these bright spots, the overall industry grade reflects an inadequate security posture that leaves most firms vulnerable to cyber threats targeting sensitive client financial information.

## How CinchOps Can Help



#### Application Security

CinchOps provides comprehensive web application security assessments and vulnerability testing to identify and remediate critical flaws in your client-facing systems and portals.



#### DNS Health

CinchOps configures and manages secure DNS settings including SPF, DKIM, and DMARC records to prevent domain spoofing and email-based phishing attacks.



#### Network Security

Our experts implement network segmentation strategies and access controls to contain threats and protect sensitive client data from lateral movement.



#### IP Protection

CinchOps monitors your network traffic continuously for compromised devices and malware communications that could damage your firm's reputation.



#### Social Engineering

CinchOps delivers ongoing phishing simulation training and security awareness programs to educate your staff on recognizing social engineering attacks.



#### Vulnerability Management

CinchOps provides automated patch management services ensuring timely security updates across all systems, applications, and network infrastructure components.