ADVANCED NETWORKS
INFORMATION TECHNOLOGY CONSULTANTS

CASE STUDY · LEGAL INDUSTRY · LOS ANGELES, CA

From Compliance Risk to Courtroom-Ready IT

How Advanced Networks helped a 52-attorney Downtown LA litigation firm achieve full ABA compliance and eliminate 11 critical vulnerabilities in 87 days.

0	87	100%	4 hrs
VULNERABILITIES REMAINING	DAYS TO COMPLIANCE	TRAINING COMPLETION	RESPONSE SLA

CLIENT SNAPSHOT

CLIENT	PRACTICE AREA	ATTORNEYS	LOCATION	TIMELINE
Harrington & Cole LLP	Litigation & Employment	52 Attorneys	Downtown Los Angeles	87 Days

THE CHALLENGE

A compliance gap no one knew existed

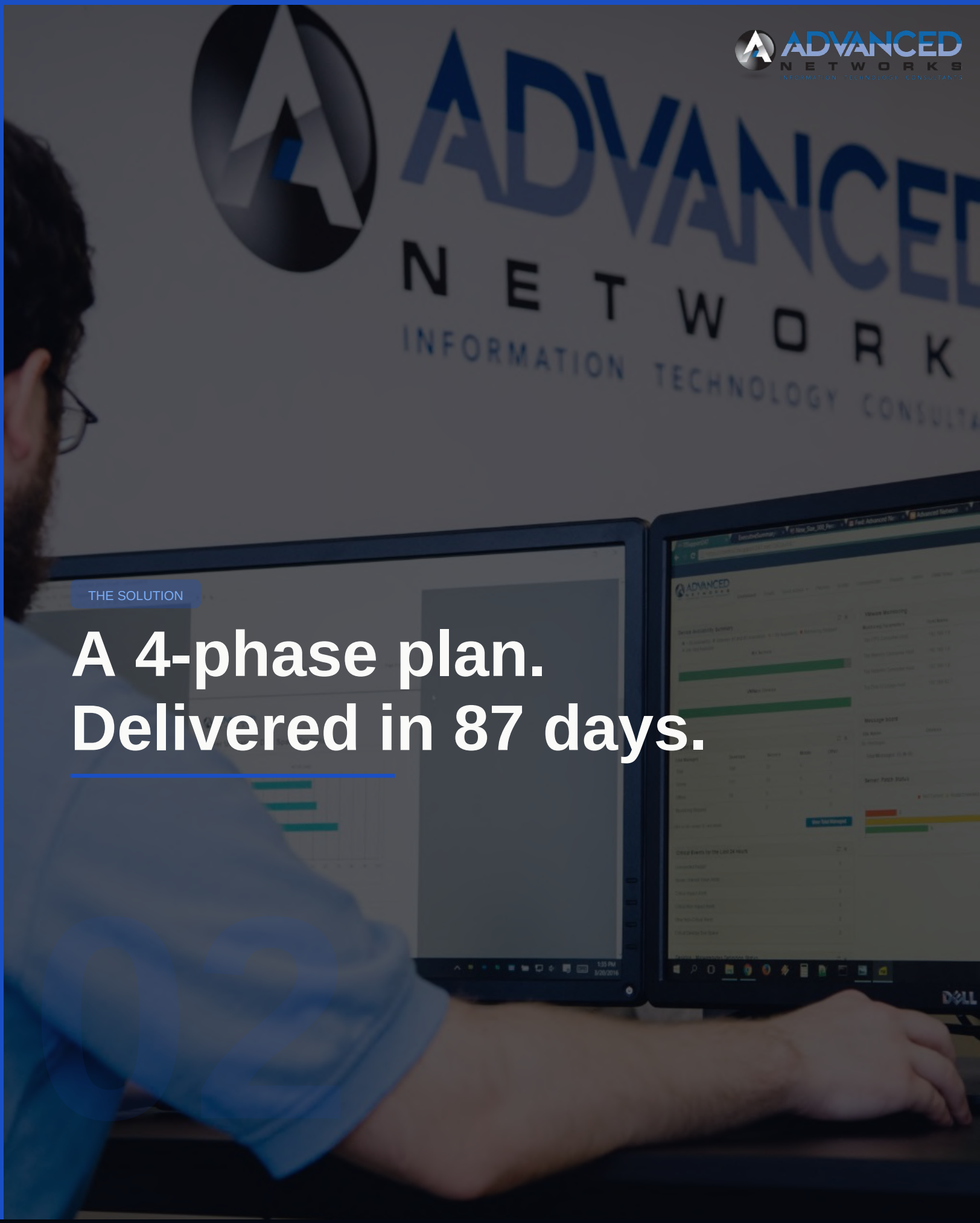
Harrington & Cole LLP had operated for over 30 years as one of Downtown Los Angeles' most respected employment and litigation practices. When a new managing partner conducted a technology review in early 2024, what she found was alarming: the firm's IT infrastructure had not kept pace with two decades of ABA ethics opinions, California Bar guidance, and evolving cybersecurity threats.

The firm was running unencrypted file shares accessible to all staff and a document management system with no audit logging — a direct violation of ABA Model Rule 1.6. A third-party penetration test revealed 11 critical vulnerabilities, including two that would have allowed an external attacker to silently access client files.

Three recently onboarded remote attorneys were accessing confidential client files over unencrypted personal Wi-Fi with no VPN — potential grounds for California Bar disciplinary proceedings. The managing partner gave the IT committee 90 days to fix it. Advanced Networks was brought in to lead the engagement.

RISK PROFILE AT INTAKE

CRITICAL	11 unpatched vulnerabilities across perimeter and endpoints
HIGH	No MFA on any attorney or staff accounts (90 users)
HIGH	Unencrypted client files on shared network drive
MEDIUM	Remote access without VPN for 3 lateral-hire attorneys
MEDIUM	No documented incident response plan on file
LOW	Outdated staff security awareness training (last updated: 2019)



THE SOLUTION

A 4-phase plan. Delivered in 87 days.

THE SOLUTION

A 4-phase remediation plan built around the ABA cybersecurity framework

Advanced Networks designed a structured 87-day engagement divided into four sequential phases, each with defined deliverables, responsible parties, and measurable compliance outcomes reviewed against ABA Model Rules and California Bar guidance.

PHASE 01

Days 1–14

Assessment & Gap Analysis

Comprehensive technical and compliance audit mapping every device, user account, and data flow against the ABA cybersecurity framework. Produced a prioritized remediation roadmap with clear ownership, timelines, and success criteria.

- ✓ Full network and endpoint vulnerability scan
- ✓ Data classification and flow mapping
- ✓ ABA Model Rules 1.1 and 1.6 gap analysis report
- ✓ Board-ready risk summary presentation

PHASE 02

Days 15–35

Critical Vulnerability Remediation

Patched all 11 critical and high vulnerabilities through existing maintenance windows, replaced end-of-life firewall hardware, and reconfigured network access controls to implement least-privilege principles across all 74 devices.

- ✓ Emergency firewall replacement and reconfiguration
- ✓ Endpoint protection rollout across 74 devices
- ✓ Network segmentation: client, staff, and guest zones
- ✓ All 11 critical vulnerabilities patched and verified

PHASE 03

Days 36–65

iManage Cloud Migration & Access Controls

Migrated the legacy document management system to iManage Cloud with matter-level access controls and full audit logging — providing the documentation trail required to demonstrate compliance under ABA Rule 1.6.

- ✓ iManage Cloud deployment with matter-level permissions
- ✓ Legacy file server decommission and secure data migration
- ✓ Full audit logging and access reporting enabled
- ✓ MFA enforced on all 90 attorney and staff accounts

PHASE 04

Days 66–87

Training, Monitoring & Ongoing Compliance

All 52 attorneys and 38 staff completed legal-specific security awareness training. The firm was enrolled in 24/7 SOC monitoring with a documented incident response plan reviewed by outside ethics counsel.

- ✓ 52 attorneys + 38 staff security awareness training
- ✓ 24/7 SOC monitoring enrollment
- ✓ Documented incident response plan (IRP)
- ✓ Quarterly compliance review schedule established

THE RESULTS

Zero vulnerabilities. 87 days.

THE RESULTS

Full ABA compliance. Zero critical vulnerabilities. In 87 days.

0 Critical vulnerabilities remaining (down from 11)	**87 days** From initial assessment to full documented compliance	**100%** Attorney + staff security training completion
4 hrs Maximum incident response time under new SLA	**$0** Regulatory fines or Bar actions since remediation	**24/7** SOC monitoring coverage across all firm endpoints

"Advanced Networks didn't just fix our IT problems — they gave us something we didn't have before: confidence. Confidence that our clients' files are protected, that we can demonstrate compliance to the Bar if we ever need to, and that our firm isn't one phishing email away from a headline."

— Managing Partner, Harrington & Cole LLP

52-Attorney Litigation Firm · Downtown Los Angeles