

CYBERSECURITY REALITY — ISSUE 2 OF 4

# Your Firm Is Already *a Target.* Here's Proof.

Cybercriminals don't chase the biggest companies anymore — they chase the least prepared ones.

**73%**

Of law firms reported a security breach in the past year.

Fewer than half have a formal incident response plan. — ABA Legal Technology Survey

**\$4.9M**

Average cost of a data breach for professional services firms.

Includes downtime, remediation, legal exposure, and client notification. — IBM 2025

FROM THE DESK OF MATRIX CONSULTING

## The Call Nobody Wants to Get

It's 7:42am on a Monday. A managing partner calls us. Their firm's server is locked. A ransom note sits on every screen. Tax returns are due in three days. Client data — confidential, privileged, regulated — is in the hands of someone they've never met.

This isn't a hypothetical. Versions of this call happen every week across Northern Virginia. And in almost every case, the firm thought it was protected. They had antivirus. They had a firewall. They had an "IT guy."

**What they didn't have was a strategy.** This week we're pulling back the curtain on what cyber risk actually looks like for professional services firms — in plain English, no jargon, no fear-mongering. Just the facts your leadership team needs.

#### MAIN FEATURE

## What's Really on Every Professional Services Pen Test Report

A penetration test is when a cybersecurity firm attempts to break into your systems the same way a real attacker would. We've seen dozens of these reports from firms just like yours. The findings are almost always the same.

#### FINDING #1

**Weak or reused passwords.** The most common entry point. One compromised employee credential opens the door to your entire network. Multi-factor authentication (MFA) stops this cold. Most firms still don't have it on every system.

#### FINDING #2

**Unpatched software.** Attackers exploit known vulnerabilities in software that hasn't been updated. Bots scan the internet 24 hours a day looking for firms running outdated systems. Patch management eliminates a staggering percentage of risk.

#### FINDING #3

**No email filtering for advanced threats.** Modern phishing attacks impersonating your bank or a managing partner sail right through standard spam filters. Business Email Compromise cost U.S. firms over \$2.9 billion last year alone.

#### FINDING #4

**Backup systems that have never been tested.** Nearly every firm has some form of backup. Very few have ever confirmed it works. A backup you've never restored from is not a backup — it's a false sense of security.

The good news: every one of these findings is fixable. None require a massive budget overhaul. They require a partner who knows what to look for and a plan to address it systematically.



*"Compliance frameworks like ABA 477R and Reg S-P don't just protect your clients — they give you a roadmap. The firms that treat compliance as a checklist get breached. The ones that treat it as a culture don't."*

— MATRIX COMPUTER CONSULTING

#### QUICK SELF-ASSESSMENT

## 5 Signs Your Firm May Be a Cyber Target Right Now

- ✓ You don't require multi-factor authentication (MFA) on email, VPN, or remote access tools.
- ✓ Your software and systems haven't been patched or updated in the last 30 days.
- ✓ You have backups — but you've never actually tested restoring from one.
- ✓ Your team has never gone through a phishing simulation or cyber awareness training.
- ✓ You don't have a written incident response plan — or you're not sure if you do.



#### NEXT WEEK

We shift from risk to opportunity — how the right IT strategy drives productivity and revenue growth at your firm.



#### FREE RESOURCE

Download our **Cyber Risk Self-Assessment for Law Firms** — an 8-question checklist showing exactly where your exposure is.



#### COMING IN JULY

Our cybersecurity webinar: *"Cyber Insurance Renewals in 2026 — What Your Carrier Now Requires."* Reserve your seat early.

## Not Sure Where Your Firm Stands?

Take our free Cyber Risk Self-Assessment and get a clear picture of your exposure in under 10 minutes — no sales call required.

**GET YOUR FREE CYBER RISK ASSESSMENT**

