

5 Moves to a More Secure Firm

A Practical Path to Go From Exposed to Defended

Your firm likely has the cybersecurity basics covered, but real protection against today's attackers or audits needs to go deeper. Follow these 5 moves to stay ahead.



Move 1



Build a Strong WISP

Your Written Information Security Plan acts as the bedrock of your entire cybersecurity strategy. Audit your plan regularly and assign an owner.

WHY? An outdated WISP is a liability and not compliant with IRS requirements.

Move 4



Back Up & Recover

Enable independent backups, run a restore drill, and ensure your retention window matches record-keeping obligations.

WHY? If you can't restore data after an incident, you've found your weakest spot.

Move 2



Control Access

Add multifactor authentication on every login, not just the main platform. Remove access for contractors or staff that have left.

WHY? Attackers don't just go after the king—they look for every undefended piece on the board.

Move 5



Close Human & AI Gaps

Implement recurring training and phishing simulations for your entire staff. Write an official AI usage policy.

WHY? 60% of breaches are due to human error. Make your staff your best line of defense.

Move 3



Bolster Devices & Email

Add endpoint detection & response (EDR) on every device. Boost your email security and enable remote wipe.

WHY? Firewalls and antivirus only stop entry-level attacks—they don't alert you to attackers who are already inside.

Master all 5 moves. Close the cybersecurity gap.

Download the free eBook.

[DOWNLOAD NOW](#)

