



Day one. Already compromised.

How we found an attacker inside a Texas law firm's Microsoft 365 tenant during onboarding

What we found	When	Outcome
An attacker with persistent access to the firm's email, hiding its own alerts	Within minutes of connecting the firm to our monitoring	Access cut off on confirmation; full timeline documented for the firm

This is not a hypothetical scenario. In September 2026, a Texas law firm engaged Counsel Cyber to manage its IT and cloud security. The first minutes of onboarding turned a routine setup into an incident response. Identifying details have been left out.

The onboarding that became an incident response

When a firm comes on board, we connect to its Microsoft 365 environment and audit it immediately: sign-in activity, MFA configuration, mail flow and inbox rules, admin permissions, and dozens of other indicators.

This time was different. Within minutes, our monitoring flagged an unauthorized actor who had already established persistent access to the firm's tenant. They weren't knocking on the door. They were already inside.

What we found

- Forwarding rules quietly sending copies of a user's email to an outside address
- An attacker-registered MFA method on a partner's account, allowing re-entry even after a password reset
- Inbox rules that marked security alert emails as read and moved them to Deleted Items
- Sign-ins from foreign datacenter IP addresses that no one had flagged

Why this matters more for law firms

A law firm's inbox holds privileged communications, client personal and financial information, and the payment and wire instructions for settlements and closings. An attacker inside that inbox can read all of it and send convincing instructions from a real firm address. The fallout reaches every client: state bar grievances, malpractice claims, notification obligations, and lost trust.

It is also an ethics issue. ABA Formal Opinion 483 (2018) says lawyers have a duty to monitor for data breaches, stop them, restore systems, and determine what happened.

What we did

- Revoked all active sessions and reset credentials on every affected account
- Removed the MFA methods the attacker had registered for re-entry
- Deleted every malicious forwarding and inbox rule
- Reviewed sign-in and mailbox audit logs to establish the attacker's access timeline, giving the firm the facts it needed to assess its obligations with counsel
- Hardened the tenant with conditional access policies, single sign-on, and 24/7 monitoring

The question to ask about your own firm

This firm thought it was secure: it had an IT provider and MFA turned on. What it didn't have was anyone watching what happened after someone signed in. If someone were inside your email right now, reading and forwarding your messages, would you know within minutes?

Find out what is happening inside your firm's email.

Schedule a confidential security assessment. (737) 325-2520 | hello@counselcyber.com | counselcyber.com
Counsel Cyber, headquartered in Dallas, Texas. Serving Texas, Arkansas, Louisiana, Oklahoma & Kansas.