



The 3 Biggest Email Security Challenges Facing Legal Organizations





Introduction

Law firms are under constant pressure to meet tight deadlines, maintain client confidentiality and protect privileged communications. And like most aspects of life with technology so deeply intertwined, the same tools that make work possible can also be significant sources of risk.

Consider something as basic as email; likely the most commonly used tool in the profession.

Despite advances in filtering and encryption, the leading cause of email-related security incidents isn't a lack of technical infrastructure—it is workforce behavior. Legal experts agree email cybersecurity and phishing remain one of the top threats to law firms of all sizes.

The challenge has evolved because the legal workforce itself has transformed. According to the 2026 Legal Industry Report, personal use of generative artificial intelligence (AI) platforms among legal professionals has skyrocketed to 69%, more than doubling from 31% in 2025. At the same time, 54% of legal professionals said their firm has provided no training on the responsible use of AI and has no plans to do so.

Static security policies cannot keep up with the complexity and speed of this modern human/AI hybrid workforce. Client trust and attorney-client privilege are on the line, and one accidental disclosure could be all it takes to lose both. To reduce risk, protect client data and improve efficiency, legal organizations must secure both their human professionals and the autonomous AI agents collaborating alongside them.

The challenge becomes how best to incorporate modern technology to reduce risk, ensure client data security and improve efficiency. A comprehensive, AI-native approach to Collaboration Security is the only way to keep a modern practice secure.

Read on to explore the biggest email cybersecurity challenges facing today's legal organizations. Learn how a cohesive approach to addressing risk can mean the difference between data (and clients) lost and a legal practice kept on firm footing.

Challenge 1: Professional Ethics and Data Protection

Why Traditional Controls Aren't Cutting It

Legal organizations operate under some of the strictest confidentiality and privilege requirements in any profession. These firms handle highly sensitive client information and are bound by attorney-client privilege, work product doctrine and evolving state bar ethics rules around technology competence.

The primary vulnerability is that legacy compliance strategies focus heavily on static systems rather than active workforce behavior. Inadvertent disclosure can dismantle a practice overnight. What's more, as AI agents take over more and more tasks, it seems only a matter of time before client-privileged emails are accidentally and autonomously shared with the wrong person.

Let's take accidentally sending privileged case materials to opposing counsel or third parties ("inadvertent disclosure") as an example. We've removed any identifying details, but this is a real story:

A lawyer believed she had emailed an attachment containing highly-sensitive medical information to one of her clients. However, she'd misdirected her email to the wrong recipient.

When the intended recipient followed up with a reminder, the lawyer realized her mistake. At this point, she panicked and lied to the client to try and buy time to rectify the mistake.

She tried (unsuccessfully) to recall the email and get the recipient to delete the message.

Unfortunately, she ended up receiving a six-month suspension from her job and had to pay a \$7,000 fine.

This goes to show how serious a simple mistake can be — and how in the heat of the moment, people can panic and make things worse.

Meanwhile, many firms are still relying on static data loss prevention (DLP) rules and legacy compliance checklists that were built for slower, paper-based workflows. These tools often miss the nuanced, real-world behaviors that create ethical risk, such as a busy associate accidentally sending sensitive client information to someone it was not meant for.

Challenge 2: Client Confidentiality and Trust

The Hidden Cost of Email Mistakes

Client relationships are built on an unshakeable foundation: the promise that sensitive information will remain confidential. Whether its merger documents, criminal case files or personal injury settlements, clients trust their attorneys to protect what matters most.

But email mistakes can shatter that trust in seconds. A misdirected message containing case strategy. An accidental “reply all” that exposes settlement terms. A phishing attack that compromises client communications. Just one of these could result in relationship-ending breaches that can destroy decades of reputation building.

The stakes couldn’t be higher. Research shows that nearly 40% of clients say they would fire or consider firing a firm that experienced a breach, and 37% said they would tell others about their experience to warn them. And in today’s competitive legal market, where client acquisition costs continue to rise, losing established relationships due to preventable email mistakes is a luxury no firm can afford.

Furthermore, cybercriminals now use generative AI to supercharge social engineering. The KnowBe4 Phishing Threat Trends Report shows that 82.6% of phishing emails now utilize AI, allowing bad actors to craft highly convincing, hyper-targeted messages that mimic legitimate corporate or legal correspondence. This creates a dangerous gap between client security expectations and the reality of how firms manage their day-to-day communications.

Yet many firms are still operating with email practices that put client relationships at risk every day. Partners forward sensitive documents without checking recipients. Associates work from personal devices with inadequate security. Support staff handle privileged communications without understanding the implications of a simple mistake.

The result? A growing gap between client expectations for data security and the reality of how most legal organizations handle email communications.

Challenge 3: Insider Risk and Information Barriers

Why Static Controls Can’t Keep Up

Insider threats in legal organizations are not limited to malicious actors. Mistakes will happen.

Often well-meaning employees operating in complex environments without clear boundaries are the cause. As modern legal teams rely on real-time communication tools like chat, video conferencing and email, often across hybrid or distributed workforces, the challenge of managing insider risk is only getting harder.

The rise of AI has only made these waters murkier. As the 2026 Legal Industry Report noted, 43% of legal professionals said their firm has no formal policy governing AI use and no plans to create one. This creates a severe Shadow AI risk, where sensitive client data is fed into public models without firm oversight, bypassing traditional infrastructure and triggering critical compliance violations.

Law firms are under strict obligations to maintain information barriers, or “ethical walls,” between matters that could have conflicting interests. These walls are critical for avoiding conflicts of interest, inadvertent disclosure and other forms of professional misconduct. State bar associations require these controls. And when things go wrong, sanctions can include suspension or disbarment.

The problem? Traditional rules-based DLP tools aren’t designed for this kind of dynamic legal environment. Static policies may block obvious red flags, but they struggle to detect nuanced risks across fast-moving, informal communication channels. And they often overcorrect, impeding legitimate case collaboration and slowing down teams trying to meet tight deadlines.

Challenge Accepted: How AI-Powered Cloud Email Security Platforms Help Law Firms Succeed

AI-powered cloud email security platforms that augment positive human behavior offer a smarter approach to legacy static policies; one that proactively prevents mistakes, automates security and delivers real transparency.

These platforms are built to prevent data leaks before they happen, without getting in the way of responsive legal service.

They continuously monitor for risky behavior, such as attaching confidential case files to emails or replying to suspicious domains. Confidentiality policies are enforced automatically, not manually, so attorneys don't have to jump through hoops just to serve their clients effectively.

And when something doesn't look right—say, a file going to a previously unknown recipient—the platform prompts the sender with a smart, just-in-time warning. It's like having a real-time safety net that doesn't slow you down.

By addressing professional ethics compliance, preserving client trust and managing insider risk before problems arise, legal organizations can reduce violations, stay agile and protect what matters most. The result? Fewer breaches, fewer sanctions and a stronger, more resilient practice built for today's challenges.

Adopting a smarter approach to client data protection delivers a powerful mix of outcomes:

- **Maintain rapid client response times** without compromising on confidentiality
- **Eliminate workflow bottlenecks** that frustrate attorneys and delay critical case work
- **Enhance client retention** by protecting sensitive information behind the scenes before issues arise
- **Build a competitive edge** by showing clients and regulators that you can be both secure and responsive

In modern legal practice, trust may still be earned by legal expertise, but it's reinforced through every secure interaction. With the right email security tools in place, legal firms can confidently protect both their data and their most valuable client relationships.

Conclusion

By addressing professional ethics compliance, preserving client trust and managing insider risk before problems arise, legal organizations can reduce violations, stay agile and protect what matters most. The result? Fewer breaches, fewer sanctions and a stronger, more resilient practice built for today's challenges.

Explore KnowBe4's Approach to Cloud Email Security

Learn More





Free Phishing Security Test

Find out what percentage of your employees are Phish-prone with your free Phishing Security Test



Free Email Exposure Check

Find out which of your users emails are exposed before bad actors do



Free Automated Security Awareness Program

Create a customized Security Awareness Program for your organization



Free Domain Spoof Test

Find out if hackers can spoof an email address of your own domain



Free Phish Alert Button

Your employees now have a safe way to report phishing attacks with one click

About KnowBe4

KnowBe4 empowers the modern workforce to make smarter security decisions every day. Trusted by more than 70,000 organizations worldwide, KnowBe4 is the pioneer of digital workforce security, securing both AI agents and humans. The KnowBe4 Platform provides attack simulation and training, collaboration security, and agent security powered by AIDA (Artificial Intelligence Defense Agents) and a proprietary Risk Score. The platform leverages 15-years of behavioral data to combat advanced threats including social engineering, prompt injection, and shadow AI. By securing humans and agents, KnowBe4 leads the industry in workforce trust and defense.

More information at www.KnowBe4.com.



KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.