Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/lawyers-and-law-firms-prime-targets-for-hackers/

LAW FIRM SECURITY

Defending Privileged Files, Deal Rooms and Trust Accounts at Law Firms

A compromised partner mailbox or document management account exposes every client whose matters it touched, and the duty to tell them turns on what the records show was reached. Preserve the audit trails before remediation and bring breach counsel in at once. Call (800) 868-8189 at any hour.

Published February 27, 2014 · Updated October 30, 2026

Primary Reference for This Guide

Start with NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response.

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

Why Law Firms Are the Ultimate One Stop Target for Cyber Syndicates and Espionage

For criminal ransomware groups, insider traders and foreign intelligence services, breaching a single corporate law firm or litigation boutique is far more lucrative than attacking dozens of individual corporations. Law firm document management systems hold non public M&A term sheets, unfiled patent applications, sensitive discovery productions for Fortune 500 clients and high value client trust and real estate escrow accounts. A breach at a law firm not only triggers severe ABA Model Rule 1.6 ethical duties and client contractual audits, but also threatens irreparable reputational harm if confidential client litigation strategy is leaked on an extortion site.

Discreet Penetration Testing and Forensic Support Built for Managing Partners

Global Digital Forensics has served AmLaw 100 firms and trial litigators for decades and understands the unique culture, ethical obligations and partner mobility of law firms. We provide discreet, partner friendly manual penetration testing across document management systems such as iManage and NetDocuments, remote partner access portals and escrow wire workflows to satisfy your corporate clients outside counsel security guidelines. If your firm or one of your clients ever experiences a suspected intrusion or email compromise, our forensic examiners respond 24/7 under the direction of counsel to contain the incident and protect client confidentiality. Our legal industry page describes the full practice.

© 2026 Global Digital Forensics, Inc. All rights reserved.

ABA Formal Opinion 483 and the Facts a Lawyer Must Determine

The ethics framework for a law firm breach is set out in ABA Formal Opinion 483, which addresses lawyers' obligations after an electronic data breach or cyberattack. The opinion concludes that when a data breach occurs "involving, or having a substantial likelihood of involving, material client confidential information", the lawyer has a duty to notify the client of the breach and to take other reasonable steps consistent with the Model Rules. It also describes a duty to act reasonably and promptly to stop the breach and mitigate the damage, and to make reasonable efforts to determine what occurred and which client information was affected. Those are factual determinations before they are ethical ones, and the firm makes them from the forensic record rather than a help desk ticket. The forensic examination exists to tell managing partners and the firm's general counsel what was actually reached.

The opinion's standard shapes the examination in a specific way. Substantial likelihood is a lower bar than proof, so the question is not only which documents the record shows were opened but which the intruder could plausibly have reached in the access window, and the report addresses both. Material client confidential information means the analysis is organized by client and matter rather than by file path, so that the firm can make a notification judgment for each client relationship. Working under the direction of the firm's breach counsel, we produce an account of the compromised accounts, the access window, the documents and matters touched, the information that was plausibly exposed and the coverage of each source. The firm's own general counsel and outside breach counsel then apply Rules 1.1, 1.4, 1.6 and 5.3 to that record. Our legal industry page describes how the practice supports firms through that process.

What Document Management and Email Records Show After an Intrusion

Law firms are better instrumented than most businesses, and the first step is confirming which instruments are turned on. Document management systems such as iManage and NetDocuments keep activity logs recording who opened, downloaded, emailed, printed or shared each document, with timestamps and session details, and those logs are the first place the examiner looks for which matters an intruder reached. Microsoft 365 adds the sign in logs that separate the attorney's sessions from the attacker's, the MailItemsAccessed and search events that show what was read and sought in the mailbox, the inbox rule operations that reveal forwarding and the SharePoint and OneDrive download events for files outside the DMS. Remote access gateways and VPN concentrators record the sessions through which the attacker arrived. Correlated, these records are how the examiner fixes the access window, the accounts involved and the documents touched, at the level of detail that client by client notification decisions call for.

Reading these records well starts with confirming their coverage, and the setting adds a legal dimension. The examiner checks whether audit logging was enabled and what retention applied, measured against the periods Microsoft publishes for each license tier, so the firm knows which window the records cover. A document opened in the DMS appears in the log, the examiner looks for documents previewed in a search result or synced to a local cache in the endpoint and sync records, and the report states which category each finding falls into. Privilege adds a dimension: the content review of exposed documents is performed under the direction of counsel to protect privilege over the firm's analysis of its own breach, and the examiner's report is

© 2026 Global Digital Forensics, Inc. All rights reserved.

written to be useful to the firm and confined to the technical facts of the access, leaving the client matters themselves to counsel. We handle these engagements with the discretion the setting demands, and our Microsoft 365 forensics page covers the mailbox sources in depth.

Running the Response With a Lean Firm IT Team

Most firms outside the largest tier run on an IT director and a managed service provider rather than an overnight monitoring team, so the response is designed for that structure. In the first hour, the affected accounts are contained: sessions revoked, passwords reset, multi factor methods re registered, unfamiliar inbox rules and application consents removed and remote access for the account suspended. In the same hour, the record is preserved: sign in logs, the unified audit log, the DMS activity logs, the gateway logs and a copy of the mailbox, exported before remediation generates new events or rotates old ones. Breach counsel is engaged before the second hour so that privilege, the insurer's notice requirements and the client notification analysis are coordinated from the start. The incident response retainer is built for this moment, because the examiner who answers already knows the firm's systems.

The analysis phase then runs along two tracks. The access track reconstructs what the intruder did across the mailbox, the DMS and any other reachable systems, and produces the access window and the list of documents and matters touched. The content track, under the direction of counsel, reviews the exposed documents for the client confidential information they contain and organizes the result by client and matter so that the firm can apply the opinion's standard to each. The output is a report to the firm's general counsel and breach counsel, and where an insurer or a client's own security team requires it, a summary suited to that audience. The structure follows NIST SP 800-61 Revision 3, and the examiner remains available for the client conversations that follow, because sophisticated corporate clients will ask their own questions about what happened.

Two audiences outside the firm shape the deliverables. The cyber insurer typically requires notice within a short window and approval of the vendors engaged, and its panel counsel may become the breach counsel directing the work, so the plan anticipates that from the outset. Corporate clients with outside counsel guidelines often have a contractual right to notice and to a summary of the incident, and their own security teams will ask pointed technical questions about the access window and the controls in place at the time. The report is written so that counsel can extract each of those summaries while keeping every other client's matters private, which is one more reason the analysis is organized by client from the start and ready when the notification letters are due.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Wire Diversion From a Compromised Firm Mailbox

Beyond the ransomware headlines, the most financially damaging law firm incident is the quiet diversion of a closing wire or a settlement payment. An intruder who has read a partner's mailbox for weeks knows the matter, the parties, the closing date and the bank, and sends revised wire instructions from the partner's own account or from a lookalike domain registered the week before. The examiner looks for the record of that scheme in the message headers, the inbox rules that hid the replies, the sign in logs that show the attacker's sessions and the registration records of the impostor domain. Our email header analyzer (evestigate.com/tools/email-header-analyzer/) lets a firm examine a suspicious message's path before the call, and the business email compromise analysis engagement reconstructs the full sequence for the firm, its bank and its insurer.

Time matters more here than in any other incident type. The firm should contact its bank and the receiving bank immediately to attempt a recall, and file a complaint with the FBI's Internet Crime Complaint Center, whose procedures for reporting business email compromise are designed around the first hours after a fraudulent transfer. In parallel, the mailbox record is preserved so that the analysis can work out when the intruder gained access, whether the firm's account or the counterparty's was the one compromised, and what else the intruder read. That determination matters for the dispute over who bears the loss, for the insurer's coverage analysis and for the client notification question, because an intruder who read the mailbox long enough to plan a wire fraud had time to read a great deal else. Our guide to the first twenty four hours of a business email compromise walks through the sequence.

Schedule a Law Firm Security Briefing

Protect your firm reputation and satisfy client security audits with confidence. Call Global Digital Forensics at (800) 868-8189 or our New York office at (212) 561-5860 to speak with a senior security engineer. The initial consultation is free.

What Document Management and Email Records Show After an Intrusion

The guide explains that law firms are better instrumented than most businesses when the instruments are turned on. This table lists the records a firm intrusion examination reads, what each shows and what the examiner confirms about it, so breach counsel can organize the analysis by client and matter. The third column records how each source is checked, including the endpoint and sync records the examiner reads for documents previewed in a search result rather than opened. The content review of exposed documents runs under the direction of counsel to protect privilege.

Document management and email records after a law firm intrusion, what each shows and what the examiner confirms.

Record	What it shows	What the examiner confirms
iManage or NetDocuments activity log	Who opened, downloaded, emailed or printed each document	Previews and local cache copies, checked on the endpoint

© 2026 Global Digital Forensics, Inc. All rights reserved.

Record	What it shows	What the examiner confirms
Entra sign in logs	The attacker sessions against the attorney's own	Retention of seven or thirty days by license per Microsoft
MailItemsAccessed and search events	What was read and sought in the mailbox	Retention of 180 days as standard per Microsoft
Inbox rule operations	Forwarding and reply suppression	The rule's creator, checked against the sign in sessions
SharePoint and OneDrive download events	Files taken outside the document system	That auditing was enabled for the period
Remote access and VPN logs	The sessions through which the attacker arrived	The retention setting on the gateway
Content review by client and matter	Which client confidential information was exposed	Run under counsel to preserve privilege

The banking industry case study shows examiners working alongside an outside professional firm and its auditors to correlate records, the discreet support under direction of counsel this guide describes for a firm.

Try the Tool Before You Call

Firms can check a suspicious client or counterpart message in minutes. Have the recipient export it as .eml or .msg, copy the full header block and paste it into the Email Header Analyzer (evestigate.com/tools/email-header-analyzer/). Read the Received hops to see where the message really entered the mail system, then read the authentication results against the domain the message claims. A closing instruction that fails SPF and DKIM for the title company domain, or that passes for a domain one letter away from it, is held for review before it reaches the escrow desk. The analyzer runs in the browser and keeps the message on your own machine, so the check itself keeps client material in house. If the message passed authentication from the real domain, assume that mailbox is compromised and call before replying.

How to Begin and What Happens on the First Call

Have ready the affected accounts and their practice areas, when and how the intrusion was noticed, what IT or the managed service provider has already done, the email platform and license tier, the document management system in use and whether breach counsel and the cyber insurer have been notified. The examiner asks whether sessions have been revoked, whether the mailbox and DMS logs have been preserved, what the accounts could reach, whether any wire or payment activity is involved and what client notification obligations the firm anticipates. Firm leadership then receive a written scope describing containment and preservation, the access and content analysis organized by client and matter, the deliverables for counsel and the insurer and the timing, with a proposal. The initial consultation is free, and the hotline at (800) 868-8189 answers 24/7.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Technical References and Further Reading

Authorities cited in this guide: ABA Formal Opinion 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack. Sets the duties to monitor, stop, mitigate, determine what occurred and notify clients after a breach involving material client confidential information, issued October 17, 2018. Microsoft Learn, Manage audit log retention policies. Documents how long Microsoft 365 mailbox and sign in audit records are kept by license level, current Microsoft documentation. FBI Internet Crime Complaint Center. The federal reporting channel for business email compromise and fraudulent wire transfers, current site. NIST SP 800-61 Revision 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management. Provides the incident response structure the engagement follows, final version published 2025.

FREQUENTLY ASKED

Questions Counsel and Security Leaders Ask About Law Firm Security

Do we have to tell clients if we cannot confirm their files were taken?

That is the firm's judgment under its ethics rules, and Formal Opinion 483 frames it around a substantial likelihood that material client confidential information was involved rather than proof. The examination narrows the question. Where the document management and mailbox logs record the intruder's sessions and what they opened, the firm can identify the clients whose matters were reached and those whose were not. Where a log was never kept, the analysis works from what the account could reach and from the other sources that recorded the session. We report both the confirmed access and the plausible exposure so breach counsel can advise on each client relationship.

Can you tell which documents an attacker opened in our document management system?

Usually, yes. iManage, NetDocuments and similar platforms log document opens, downloads, emails, prints and shares with the user, time and session, and correlating those entries with the intruder's session windows from the identity logs separates the attacker's activity from the attorney's. The examiner confirms retention and configuration first, since some firms log only certain actions or keep logs for short periods, and checks previews and cached copies on the endpoint. We export the logs on the first day, document where the record begins and ends and organize the results by client and matter for the notification analysis.

Our trust account wire was diverted. What should we do right now?

Call the sending and receiving banks immediately to request a recall and a freeze, report the transfer to the FBI's Internet Crime Complaint Center, and engage breach counsel. Keep everything in the mailbox, and reset passwords once the sessions have been revoked and the logs exported, because the record of how the intruder operated is what the banks, the insurer and the dispute over the loss will turn on. Then have the mailbox and identity logs analyzed to establish when access began, whose account was compromised and what else was read. Every hour matters for recovery.

© 2026 Global Digital Forensics, Inc. All rights reserved.

How does a penetration test protect the attorneys' working day?

The rules of engagement are written so the attorneys keep working normally. Testing of the document management system, remote access portals and email environment is scheduled with the IT director, uses dedicated test accounts and keeps availability and client documents untouched. The attorneys' day runs as usual, and a phishing simulation is included when the firm chooses one and agrees it in advance. The report is delivered to firm leadership and IT and kept within that group, and it is written to serve the outside counsel guidelines that corporate clients increasingly require firms to satisfy.

What do outside counsel security guidelines usually require of a firm?

They vary by client, but common elements include multi factor authentication on all remote access, encryption of data at rest and in transit, access controls and logging on the document management system, periodic penetration testing with results available for review, a written incident response plan with notification commitments measured in hours or days, vendor management for the firm's own providers and security awareness training. Clients increasingly ask for evidence rather than attestations. A firm with a dated testing record and a tested response plan answers those questionnaires quickly, and we help firms build both.

Web Addresses for the Sources Cited

1. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response: https://csrc.nist.gov/pubs/sp/800/86/final
2. ABA Formal Opinion 483: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf
3. NIST SP 800-61 Revision 3: https://csrc.nist.gov/pubs/sp/800/61/r3/final
4. Internet Crime Complaint Center: https://www.ic3.gov/
5. Microsoft Learn, Manage audit log retention policies: https://learn.microsoft.com/en-us/purview/audit-log-retention-policies

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.