5 IT Failures That Trigger **Malpractice Claims**

What law firms often discover after the damage is already done. Prepared for law firms by an IT provider that works exclusively with legal practices.

Malpractice claims are rarely the result of poor legal strategy alone.

Increasingly, firms face exposure because of missed deadlines, lost evidence, data breaches, or system outages. In many of these cases, the root cause is not legal error. It is an IT failure that went unnoticed until it was too late.

Courts, clients, regulators, and cyber insurers now expect law firms to demonstrate digital competence and operational resilience. “Technical issues” are no longer viewed as a valid explanation when client interests are harmed. This brief outlines five IT failure patterns that have directly contributed to malpractice claims, disciplinary actions, or client lawsuits against law firms. This document is not intended to alarm. It is intended to inform.

Failure #1: Backup Systems That Silently Fail

WHAT FIRMS BELIEVE:

- Backups are running
- Data is protected
- Redundancy exists

WHAT ACTUALLY HAPPENS:

- Backup jobs fail quietly
- Error alerts are ignored or never configured
- No one regularly tests restores
- The problem is discovered only after a ransomware attack, server failure, or accidental deletion

MALPRACTICE EXPOSURE:

- Loss of client evidence
- Inability to produce discovery materials
- Court sanctions or adverse rulings

WHY THIS BECOMES A CLAIM:

Courts increasingly view the failure to safeguard and recover client data as negligence, not bad luck. Clients argue that the loss was preventable, and in many cases, they are correct.

Failure #2: Missed Deadlines Due to System Outages

WHAT FIRMS BELIEVE:

- Downtime is rare
- Staff can work around outages

WHAT ACTUALLY HAPPENS:

- Email or document systems go down during filing windows or trial preparation
- No tested failover environment exists
- Remote access fails at critical moments
- Staff lose access to calendars, case files, or e-filing systems

MALPRACTICE EXPOSURE:

- Missed court deadlines
- Late filings
- Loss of appeal rights

WHY THIS BECOMES A CLAIM:

Judges and clients do not accept IT outages as justification for missed obligations. Firms are expected to plan for continuity and access under adverse conditions.

Failure #3: Email Compromise and Unauthorized Disclosure

WHAT FIRMS BELIEVE:

- Firewalls are sufficient
- Staff know how to spot phishing

WHAT ACTUALLY HAPPENS:

- Phishing attacks lead to mailbox access
- Attackers monitor conversations without detection
- Sensitive client communications are exposed or altered

MALPRACTICE EXPOSURE:

- Breach of client confidentiality
- Privilege waiver arguments
- Ethical complaints and bar scrutiny

WHY THIS BECOMES A CLAIM:

Email is a primary client communication channel. Basic protections such as multi-factor authentication and monitoring are now considered part of the standard of care.

Failure #4: Document Retention and Legal Hold Breakdowns

WHAT FIRMS BELIEVE:

- A retention policy exists
- Archived data is covered

WHAT ACTUALLY HAPPENS:

- Retention policies conflict with legal holds
- Files are deleted, overwritten, or become unrecoverable
- Discovery requests expose gaps in recordkeeping

MALPRACTICE EXPOSURE:

- Spoliation claims
- Court sanctions
- Adverse inference rulings

WHY THIS BECOMES A CLAIM:

Written policies alone are insufficient. Firms are expected to align IT systems with their legal and ethical obligations and enforce those controls consistently.

Failure #5: Vendor Risk and Unpatched Systems

WHAT FIRMS BELIEVE:

- Software vendors manage security
- Updates happen automatically

WHAT ACTUALLY HAPPENS:

- Practice management or billing systems remain unpatched
- Third-party tools introduce vulnerabilities
- No one owns vendor oversight or accountability

MALPRACTICE EXPOSURE:

- Data breaches
- Client notification requirements
- Reputational damage

WHY THIS BECOMES A CLAIM:

Responsibility for protecting client data cannot be outsourced. Firms remain accountable for failures caused by third-party vendors.

The Common Thread

Across these failures, three patterns consistently emerge:

- The firm believed it was protected
- The issue went unnoticed until damage occurred
- The exposure was preventable

These are not rare edge cases. They are recurring failure modes seen in law firms of all sizes.

Identify Your Firm's Exposure

Understanding risk before an incident occurs is far less costly than responding afterward. A confidential, law firm–specific IT risk review can help identify which of these exposures apply to your environment.

- No obligation
- Designed specifically for law firms

Request a confidential IT risk review to identify potential exposure before it becomes a claim.

P: 262.288.1501 | **E:** info@n8its.com | **W:** www.n8its.com