Incident Response Has Become a Law Firm Survival Skill

By Michael C. Maschke, Sharon D. Nelson, Esq., and John W. Simek

Cyber incidents are no longer rare, hypothetical events reserved for global corporations and household-name brands. Today, law firms of every size are squarely in the crosshairs. Ransomware groups, credential thieves, and organized cybercriminals understand exactly what law firms hold: sensitive data, privileged communications, financial leverage, and time-critical operations.

Recent 2025 Mandiant incident response research highlights a reality many companies still find hard to accept: most breaches don't fail due to a lack of technology. They fail because organizations are unprepared to respond under pressure.

In other words, it's not just what you buy. It's what you practice.

The "Break Glass" Moment Comes Fast

Across countless real-world incidents, the same issues keep recurring: outdated response plans, unclear leadership roles, slow decision-making, and confusing communications. When attackers breach a network—often using stolen credentials rather than sophisticated exploits—organizations waste valuable hours just trying to figure out who is in charge and what should be done first.

In cyber response, delays compound damage. Data exfiltration, lateral movement, and ransomware deployment don't wait for committee meetings.

For law firms, those delays are especially risky. They can lead to loss of client trust, increased regulatory scrutiny, ethical issues, and potential malpractice claims all within the first 24 to 72 hours after discovery. The choices made during that critical period determine the entire course of what happens next.

What a Real Incident Response Plan Looks Like in 2026

A modern incident response plan is no longer just a single document tucked away in a shared folder. It is a dynamic operational playbook based on realistic attack scenarios. Strong programs now focus on:

- Scenario-specific playbooks for ransomware, phishing, insider threats, and data theft
- Clearly defined leadership and authority spanning IT, executive leadership, legal counsel, cyber insurance, and communications

- Centralized, automated detection where alerts and endpoint activity are correlated in real time
- Regular tabletop exercises where firms rehearse breaches under controlled pressure
- Post-incident reviews that drive fundamental improvements rather than quiet documentation

The key shift is treating incident response like emergency management rather than treating it like IT troubleshooting. When a breach occurs, firms must move instantly from "business as usual" into structured crisis mode.

Why This Matters More for Law Firms Than Most Industries

Unlike many businesses, law firms operate under strict confidentiality and fiduciary obligations. A ransomware attack doesn't simply disrupt operations; it can also compromise attorney-client privilege, court deadlines, escrow accounts, and regulatory compliance across multiple jurisdictions simultaneously. Despite this, many firms still invest heavily in prevention but underinvest in response.

It is common to see detailed business continuity plans paired with outdated or barely tested cyber response protocols. That gap represents one of the most dangerous blind spots in legal risk management today. Cyber insurance may help cover recovery costs, but it cannot undo reputational damage or restore client confidence once sensitive matters are exposed.

Preparedness Is a Leadership Issue, not a Technology Issue

Perhaps the most critical insight from recent incident response research is this: The companies that recover quickly are not those with the most tools—they are the ones whose executives, partners, IT teams, and outside counsel have already practiced their roles before stress, confusion, and public pressure arise. Preparation does not stop breaches from happening. It limits the damage when they do occur.

Cyber incidents are no longer unexpected events. They are statistically inevitable. The differentiator is no longer whether a firm will experience a breach, but how quickly and competently it responds when that moment arrives.

Every firm should be able to answer this question without hesitation:

If ransomware detonated right now, who leads our response in the first 30 minutes?

If the answer is unclear, the plan isn't ready. And in today's legal environment, incident response is no longer just a compliance exercise but a core survival skill.

Michael C. Maschke *is the President and Chief Executive Officer of Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity, and digital forensics, and he has co-authored 14 books published by the American Bar Association. He can be reached at mmaschke@senseient.com.*

Sharon D. Nelson *is the co-founder of and consultant to Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com.*

John W. Simek *is the co-founder of and consultant to Sensei Enterprises, Inc. He holds multiple technical certifications and is a nationally known digital forensics expert. He is a co-author of 18 books published by the American Bar Association. jsimek@senseient.com.*