The Next Legal Nightmare: Compliance Risks of Unmanaged AI and SaaS Access

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

The new identity crisis for law firms isn't philosophical; it's digital. A recent survey of 1,000 CIOs and CISOs reveals a concerning trend: over 60% of enterprise SaaS and AI applications lack governance. That's not just an IT oversight—it's a legal risk waiting to be exploited.

This revelation demonstrates that most organizations are losing track of who has access to what, when, and why. The result? Excessive permissions, orphaned accounts, and unsanctioned AI tools operating in the shadows—all of which create a minefield of regulatory and litigation exposure.

The findings are shocking:

- Nearly half of former employees still have access to internal systems.
- One in two users has more access than they need.
- Just 15% of companies have implemented just-in-time (JIT) access.
- Only 5% follow an accurate least-privilege model, despite the well-known benefits.

When identity management fails, the consequences ripple far beyond the IT department. In a data breach litigation, discovery will quickly reveal whether appropriate controls were in place. Regulators will ask why terminated employees were still able to download sensitive data. Opposing counsel will scrutinize whether an unsanctioned AI integration accessed privileged or confidential information.

Implications for Attorneys and Their Clients

If your clients operate in regulated sectors—such as finance, healthcare, legal, or government—unmonitored access to systems and data poses a compliance nightmare. Identity governance failures can lead to:

- Violations of HIPAA, GLBA, and GDPR
- Breach of contract or fiduciary duties
- Evidence of negligence in cybersecurity litigation
- Erosion of attorney-client privilege through careless AI adoption

The most alarming part? The risk is already widespread, and most organizations don't realize how exposed they are until it's too late.

Practical Steps Law Firms Should Take to Reduce Identity Risk

Law firms must take a hard look at their own internal identity and access management (IAM) practices. Firms cannot afford to rely on outdated or informal controls, given the sensitivity of the data they possess. With increasing regulatory scrutiny and the rise of insider threats, it's critical for firms to proactively secure who has access to what, and when.

Here are five key areas where firms should focus their efforts:

1. Automate Access Controls
Modern identity governance solutions can automate provisioning, deprovisioning, and access reviews in real time.

2. Enforce Least Privilege and JIT Access
Implementing time-limited or contextual permissions reduces both human error and the attack surface.

3. Audit Internal Policies and Documentation
Review onboarding, offboarding, and access review procedures for consistency and legal defensibility.

4. Update Contracts and Vendor Agreements
Ensure third-party agreements include access controls, monitoring obligations, and breach notification clauses.

5. Encourage Legal–IT Collaboration
Legal and IT leaders must collaborate on risk assessments, breach response plans, and governance structures.

The Legal Stakes Are Rising

Unchecked access and shadow IT are symptoms of a deeper governance issue—and in today's AI-enabled business world, they're also liabilities. When breaches occur, the questions are not all technical:

- Who had access?
- Why didn't access get revoked?
- Was sensitive data protected by policy, or exposed by oversight?

These are legal questions. And in many cases, courts and regulators will not be sympathetic to "we didn't know."

Identity management has long been viewed as an IT administrator's responsibility. But as AI tools proliferate and compliance burdens grow, identity governance must become a legal priority. For law firms, this is an opportunity to step in proactively. Understand that effective IAM is not just good hygiene—it's a vital risk management strategy. Law firms must treat excessive permissions and orphaned accounts as material threats, not mere technical glitches.

***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.*