LEGAL
MANAGEMENT
THE MAGAZINE OF THE ASSOCIATION OF LEGAL ADMINISTRATORS

Cloud Security … A Competitive Advantage?

We should enjoy the cloud and related hype while we can.

JOBST ELSTER
Head of Content & Legal Market Strategy, InsideLegal

In my estimation, we are a few years away — even in legal — from native cloud applications and services making up a vast majority of our technology landscape, at which point saying "cloud" will be like adding "www" to a website address.

A recent cloud adoption survey by data security firm Bitglass revealed that among the 100,000 cross-industry businesses sampled, total cloud adoption increased from 28 percent in 2014 to 48 percent in 2015. This is not solely a U.S. trend. According to the Cloud Industry Forum's latest cloud adoption survey, 78 percent of U.K. enterprises are using off-premise services (AKA cloud), with the forecast to exceed 85 percent within the next two years.

The cloud is a bit like social media in legal — no matter how hard we try to ignore it and dismiss its viability, it just won't go away. In fact, cloud technologies have been around for a while, often unbeknownst to consumers and business users alike. For example, Hotmail launched in 1996; Salesforce.com, the "OG" Software-as-a-Service (SaaS) platform, started in 1999, as did NetDocuments, the legal market's first native cloud document and email management system.

Today, even the classic anti-cloud excuse of data security is fading away. According to the International Legal Technology Association (ILTA)'s 2015 Technology Survey, a mere 4 percent of law firm respondents cited "cloud apps/data security" as a major security challenge compared to the concern of "balancing security with usability" (31 percent).

The cloud is a bit like social media in legal — no matter how hard we try to ignore it and dismiss its viability, it just won't go away.

SECURITY STANDARDS

It's time to think out cloud — can we develop **cloud security best practices for all legal professionals?** That's what the Legal Cloud Computing Association (LCCA), a consortium of the leading legal cloud computing providers, is shooting for with the recent release of its *cloud security standards doctrine*.

The new draft guidelines set standards for a range of issues related to law firms using cloud computing services, including:

- Geographic data location, data redundancy and disclosure requirements
- Encryption and data integrity best practices
- Data loss prevention measures and data retention policies
- End-user authentication and access controls
- Terms of service and privacy policies

Jack Newton, Chief Executive Officer (CEO) of cloud practice management provider Clio and President of the LCCA, feels the standards will give the legal profession certainty as to the specific steps taken by technology vendors in keeping their data private. They will also provide the basis for a common set of standards that state bar associations and law societies will support. According to the LCCA, the initial goal is to have a version 1.0 set of standards published during the ABA Law Practice Division's ABA TECHSHOW this March.

So do the cloud standards proposed by the LCCA go far enough? What about law firm clients and their security requirements?

In 2014, *The Wall Street Journal* first reported on the proactive move by big banks to tighten cyberattack defenses by subjecting their outside counsel to tighter security audits and system compliance checks. As hackers and others with malicious intent evolve and innovate in order to gain access to confidential data, more than ever it's the vendors' and firms' responsibility to stay ahead of these threats. Many clients demand it. Plus, security audits are increasingly subjecting law firms to proof of enforcement.

So what can technology vendors, in particular, do to stay agile and adapt to these changing regulations and market factors?

I spoke with David Hansen, NetDocuments' Director of Governance and Compliance for an insider's perspective.

"Since security and compliance are not a static destination but rather an evolving improvement continuum, it is imperative that software improves through periodic releases and that the security and compliance measures keep pace with the software and delivery model," says Hansen. "The end result is not just [SaaS], but also Security-as-a-Service."

It's a service that more law firms are taking advantage of because they understand that cloud companies are best equipped to interpret, comply with and ideally exceed global security standards addressing cryptography, flexible storage options for data sovereignty and information governance, and compliance (e.g., certifications such as ISO 27001, SOC 2 Level 2, SOC 2+, SEC/FINRA, and HIPAA security compliance).

To that end, Hansen mentioned that NetDocuments law firm customers are now increasingly turning to the cloud provider to help them comply with their clients' security audit demands.

"It makes sense," he says. "We have the expertise and knowledge, and it's in our own interest to make sure our customers are compliant based on heightened global security standards."

So can firms turn security and compliance demands into a competitive advantage? Or as Handshake Software Chief Executive Officer Doug Horton ***suggests***, should security be considered an add-on — depending on client security needs — and charged for like airline baggage fees?

We'll pay for ISO certification, but SOC2 Level 2 compliance is going to cost you extra.

ABOUT THE AUTHOR

Jobst Elster is InsideLegal's Head of Content and Legal Market Strategy. He has served as a legal market strategist for the last 17 years, advising companies entering the legal market, involved in mergers and acquisitions, and expanding strategic operations overseas. Elster regularly writes and speaks on legal technology, market research and leveraging market data, technology innovations and futures, legal marketing and big data.

Email
Twitter