Written by
Heidi Salow

Keeping your intellectual property in the cloud

Heidi Salow, vice president at Thomson Reuters, shares best practices for securing IP assets and confidential data in the age of digital storage

Data, data, everywhere — organizations are flooded with it. Thanks to a perfect storm of an increased reliance on enterprise resource planning (ERP) software, combined with low-cost storage, corporations are collecting petabytes of data on everything from consumer buying patterns to supply chain logistics.

Because few firms have endless IT support or acres of real estate for server farms, they're increasingly turning to cloud computing services (the "Cloud") for hosted software and storage. In fact, the Cloud is becoming so prevalent that industry experts project that, by 2016, it will account for the bulk of corporate IT spending. But housing everything on a virtual server comes with its own set of risks, from privacy and security breaches to back-up capabilities, which could spell disaster when it comes to protecting a company's most critical data.

That creates a conundrum for the IP department, which is responsible for, arguably, the most sensitive data in the corporate treasure trove — the vast portfolio of patents, trademarks and other intangible assets that are relied upon to drive future growth. On the one hand, the Cloud offers huge value and flexibility over a locally-installed IP management system. Cloud-based solutions allow for seamless collaboration between teams, little to no support from the internal IT team and automatic, system-wide upgrades that don't require any hardware commitment. On the other, the move to the Cloud requires a leap of faith that an outsourced vendor will deliver the same or better security (and related privacy) than that of one's own, locally-installed systems.

James Bond not required

Given all of the headlines focused on data privacy of late, it's not surprising that visions of international espionage tend to dance in people's heads. In our work implementing the Cloud-based versions of our Thomson IP Manager solution, which allows clients to maintain their vital IP portfolio data virtually, we encounter concerns about personally identifiable data and confidential corporate data on a daily basis.

The mundane reality is that with a well-reputed vendor, your data is at least as safe as if it were internally stored — if not more so. At Thomson Reuters, we have a team dedicated to global privacy compliance and we keep abreast of the constantly evolving laws, regulations and standards. We have data centers in several geographic areas which meet established international standards for data security. To provide our clients with truly cost effective and scalable Cloud-based solutions, we've also developed a series of best practices for transitioning out of the locally-hosted universe.

Eliminate manual processes

A primary goal for any firm storing sensitive information on the Cloud must be to reduce the number of unstructured human interactions with that data. Consider the risks associated with information sent via unsecured email, or data printed and manually filed in a cabinet. In these scenarios, confidential data, including intellectual property assets, could easily be forwarded to an unauthorized viewer.

By adopting a complete electronic process, companies can greatly reduce the number of people who touch confidential or sensitive information and mitigate the risk of leakage. Robust electronic data collection and processing systems also allow those submitting such information to do so in a secure and controlled environment that error-checks all information entered, prohibits the submission of incomplete forms and encrypts all stored data.

Create chain of custody

This highly choreographed handling of data from initial input through storage, analysis and risk reporting is essential for security, but it also serves another purpose -- the ability to quickly and accurately re-create a chain of custody. Even companies that make a good faith effort to protect their confidential and sensitive data and track the source(s) of such data sometimes fail to keep a digital trail of who had access to it.

Companies collecting and storing confidential or sensitive data in the Cloud need to maintain an auditable record history that is date- and time-stamped with each user's actions logged throughout the process. This information provides a clear, easy-to-follow chain of custody.

Control access rights

Another key to data security is having the flexibility to provision users in such a way that different people can access and manipulate data depending on their role within an organization. Administrators can dramatically reduce the risk that confidential data will fall into the wrong hands by limiting access based on job functions and assigned projects -- so that certain permissions are assigned only to people whose job functions necessitate specific functionality or data within a system. In addition, other controls can be put in place — such as not allowing local data storage, report printing or access from remote IP addresses.

For example, while Thomson IP Manager lets key stakeholders collaborate through stages of the IP lifecycle, including patent and trademark innovation, prosecution, protection and maintenance workflow processes, such collaboration is permitted only for individuals specifically designated by the organization.

Toward a zero-hand-off future

With a constantly-changing IP landscape, protecting your assets is of paramount importance. As we march towards an electronic world that's increasingly cloud-based, a good way to reduce risk is to build an electronic chain of custody that breeds consistency in data collection, storage, access and reporting. Though the mere mention of data security and privacy is still daunting, the process becomes a lot more predictable for those who have the foresight to plan for worst case scenarios and build the infrastructure they need to lessen uncertainty.

Heidi Salow is Vice President & Senior Privacy Officer at Thomson Reuters