Managing **Information Risk** with **Lateral Hires** and **Lawyer Departures**

Is your firm properly handling its information management obligations when lawyers join or leave the organization? It's no secret that most firms have seen personnel changes in recent years, most notably in response to the economic downturn. In this context, industry trends, including new rules of professional responsibility, case law and government regulations, underscore the growing importance of diligently addressing confidentiality requirements tied to personnel movement. Firm risk and IT teams have critical roles to play in preparing and protecting their organizations when there are lateral hires or lawyer departures.

Open the Door, Close the Screen

Today, lawyer mobility is a fact of life and a common occurrence. But lateral hires often create conflicts of interest that must be resolved. In many instances, firms can address these conflicts by setting up ethical screens. In some of those situations, clients or former clients must consent and sign waivers. However, in an increasing number of U.S. jurisdictions, consent isn't necessarily required so long as ethical screens are employed.

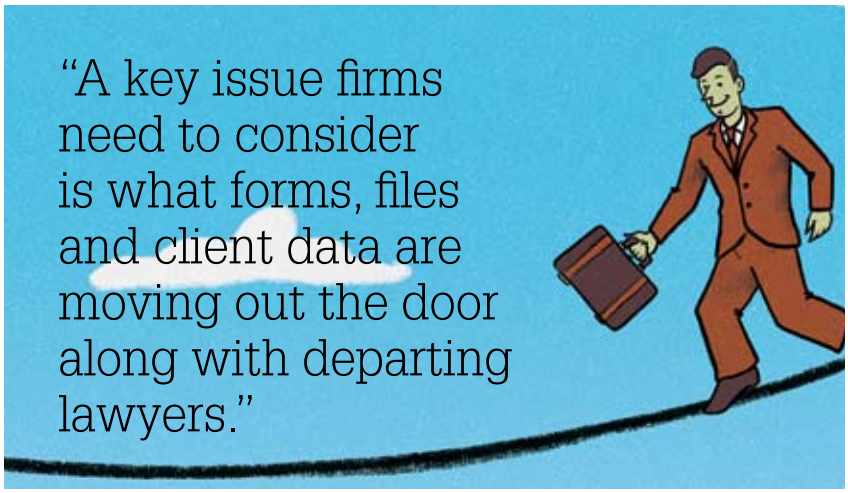
Whenever a firm relies on an ethical screen to address a conflict stemming from a lateral hire, it's vitally important that the organization be prepared to withstand a disqualification motion from opposing counsel. Successful screening defense hinges on the ability to demonstrate adequate internal policies coupled with timely and effective confidentiality controls. These controls must restrict the ability of affected parties to access relevant information internally.

The Evolution of Screens

Originally, ethical screens were primarily "policy-only" instruments. To satisfy their professional obligations, firms distributed memoranda and relied on the personal diligence of individuals to avoid inappropriate communication or information-sharing with designated parties. As a further check, organizations also might have restricted access to physical files by attaching "red dot" stickers to prevent accidental disclosure.

Today, the pervasive use of technology renders such approaches obsolete. Most information is created and stored electronically, and new search tools surface vast quantities of client and firm information for any interested attorney or staff member.

In response, industry standards for confidentiality have changed. Policy-only or manual security-enforcement processes have been replaced with automated notification, enforcement and reporting. These changes were driven partially by clients, who insisted on documented, auditable screening procedures before granting waivers. They've also been shaped significantly by the legal community itself, through changing jurisdictional rules of professional conduct and a growing body of more stringent and explicit case law.



Substandard Screening Sabotages Success

Consider recent examples of faulty screening. In 2009, an AmLaw 200 firm was disqualified, not for failing to screen a conflicted lateral hire, but for failing to set up the screen in a timely manner. In this ruling, the judge cited delay as the deciding factor invalidating the screen, and highlighted case law setting out the need for screens to be demonstrably effective "such that there can be no doubts as to the sufficiency of these preventive measures."

In another 2009 decision, a judge affirmed a screen and denied a disqualification motion, but instructed counsel to implement extra protections by extending security controls to the firm's time entry application and regularly circulating internal reminders regarding the screen.

Screening Standards Are Strict

These stories illustrate an important lesson — appearances matter. Firms face potential disqualification if screens are not timely, access controls are insufficient or internal notification measures are deficient. For a screen to be invalidated, no evidence of actual disclosure is required. If it is possible for an individual to access or be presented with restricted information, even by accident, that

This article was first published in ILTA's March 2010 issue of *Peer to Peer* titled *"Risky Business"* and is reprinted here with permission. For more information about ILTA, visit their website at www.iltanet.org.

possibility alone casts doubt regarding the sufficiency of the screen. This is especially true when peer firms are employing more stringent protective measures.

With an increasing body of case law enumerating specific screening requirements, the days of "on your honor" and "red dot" approaches to ethical screening have passed. Today firms must use effective, timely and demonstrable measures they can report on in response to client inquiry or court challenge.

Rules and Expectations Are Changing

Court decisions aren't alone in shaping law firm screening standards and practices. Industry rules also have evolved, largely in response to the realities of lateral movement among law firms. In the United States, the American Bar Association (ABA) recently updated its model rules to allow screening without client consent. More important, the new rules accept unilateral screening but mandate additional enforcement, notification and tracking requirements.

Other countries have similar, and often more stringent, rules and requirements. In the United Kingdom, screens are called "electronic information barriers," and are an acceptable way to manage confidentiality. In Canada, the Canadian Bar Association (CBA) adopted more permissive screening rules in 2008. Their recommendations highlighted the importance of screening technology:

> "*Sophisticated confidentiality screen software can now restrict access to electronic documents to those who are permitted access pursuant to established confidentiality screens. Confidentiality screen software can be linked with time-entry software to ensure that only those who are authorized to participate in a matter can docket time to the matter. With the advent of these computerized monitoring and security systems comes much more assurance that client confidentiality has been protected and that information has not been improperly accessed.*"

The Industry Confidentiality Management Trend

Today, some firms still forgo rigorous confidentiality enforcement measures and live with the resulting uncertainty and risk. Others employ tactics they perceive to be "good enough." These may include distributing memoranda and manually configuring initial document security controls. However, such approaches do not address the data management, notification and ongoing tracking, maintenance and reporting implemented by many firms across the industry.

No firm wants to find itself in the unwelcome position of disclosing or explaining an infraction to clients, the court, the press or a regulatory body, which is why most firms take all the steps necessary to enhance the practices, standards and protections they rely on to manage confidentiality. It's a prudent response to an important risk issue that no organization is immune to.

Firms seeking to follow industry-standard confidentiality management practices face a burdensome set of requirements. Manual efforts cannot achieve the same compliance levels as automated approaches. Organizations seeking to put in place the strongest risk protections available look to confidentiality management technology. According to the 2009 Law Firm Risk Management Survey, the vast majority of NLJ 250 firms use some measure of electronic and policy controls to limit access to information subject to ethical screening or other confidentiality rules.

Managing Risk When Lawyers Leave

Lawyer departures can create significant expense for law firms, including direct costs from client departures and indirect costs from lost relationships and knowledge. And the risks stemming from departures can actually exceed the cost of a lost book of business. A key issue firms need to consider is what forms, files and client data are moving out the door along with departing lawyers.

Competitive and even malpractice dangers are fueled when client information is transported prior to official consent, or when attorneys take work product from non-migrating clients or from the firm's knowledge management library.

It's not uncommon for laterally departing lawyers to remove files because "they're sure" that clients will be moving with them to new firms. But considering the confidentiality, records management and other areas of risk, even innocent mismanagement of information can create serious repercussions for clients and firms alike.

For example, if the movement of information circumvents a firm's records management and retention processes, documents that should be destroyed might not be. With clients increasingly mandating confidentiality and other information management standards, unmanaged movement can put a firm in violation of outside counsel guidelines prescribing records management practices. It also creates the very real possibility that a client involved in litigation could find that discoverable information, once thought destroyed, has resurfaced. Similarly, firms investing heavily in knowledge management and the creation of a "best and blessed" work product and precedent repositories would not know that material was making its way to their competitors.

The Realities of Policy vs. Practice

In many instances, existing firm policies explicitly forbid lawyers from unilaterally taking information with them when they leave. However, attorneys sometimes either aren't aware of these

This article was first published in ILTA's March 2010 issue of *Peer to Peer* titled *"Risky Business"* and is reprinted here with permission. For more information about ILTA, visit their website at www.iltanet.org.

policies, or they think the policies don't apply to their situations because they expect (or hope) to bring their clients with them. But it's important to remember that clients own their own files, and that unauthorized movement creates potential repercussions for clients, firms, departing attorneys and even the organizations they join. Therefore, it is vitally important for firms to keep close tabs on how departing attorneys and staff treat sensitive information to ensure that they honor professional and ethical obligations.

Data Leakage Risks Created by Technology

A decade or two ago, before the pervasive use of technology to create, disseminate and manage work product and client information, inappropriate data movement was hard to miss. In that world, paper was the dominant medium, and large-scale, unauthorized removal of data was easier to catch. A massive checkout of hard-copy materials was much less likely to go unnoticed. Files had to be retrieved, copied and moved using dollies and handcarts, often with the help of records or other support staff.

Today, large quantities of client and internal firm information can be copied quickly and moved covertly. Tools like e-mail, document management, search and KM applications provide firms with tremendous benefits in terms of productivity and knowledge-sharing. But these benefits also come at a cost; with easy access and limited oversight, individuals can fit the equivalent of a library on a thumb drive and walk out the door. That innocent-looking iPod may be transporting a great deal of intellectual property.

Combating Data Leakage Risks

Given the risks associated with inappropriate removal of client and firm information, firms should think carefully about the steps they're taking to protect themselves and start by assessing existing rules and procedures. A survey of stakeholders from key departments (IT, records, HR, risk), noting any inconsistencies or disconnects between policy and practice that they identify, is a good way to begin.

This analysis provides the basis for internal education and training efforts. Individuals often inappropriately move information due to a mistake or misunderstanding, not malfeasance. By using policy management and notification mechanisms, firms can ensure lawyers and staff better understand the rules and expectations. Any education effort requires controls to ensure policies have been read and acknowledged. Similarly, organizations should train "unwitting accomplices," such as helpdesk staff and records stakeholders, to look for warning signs of unusual activity. Training them to follow a clear escalation process frees them from having to police lawyers without proper support. For example, a lawyer request to the helpdesk to collect and package their entire e-mail history might warrant external review.

Technology can also play an important role. By using tools that flag abnormal activity in document management libraries, firms can receive notification when user behavior strays outside the ordinary. Unusually high document check-out volume is often a warning sign of an impending lateral departure.

These alerts can be set based on general thresholds, or to watch a specific office when departures are suspected or pending. Abnormal activity alerts provide firms with opportunities for early response. With these early warnings, several firms have successfully intervened and prevented imminent lateral departures. This approach is relatively painless, as it is transparent to attorneys and end users and, therefore, doesn't raise any internal concerns.

Conclusion on Managing Risk Tied to Lawyer Movement

Any time a lawyer joins or leaves the firm, the organization must take care to address risk management requirements tied to information access and movement. Today, the explosion of electronic information technology has increased the opportunity for error and oversight. However, software also provides firms with new resources. In recent years, many firms have adopted confidentiality tools to mitigate these risks.

As firms embrace more thorough approaches to compliance, they've created stricter *de facto* industry standards. At the same time, court, client and insurance expectations have also risen. Now more than ever, it is critically important that IT and risk staff take sufficient measures to enhance their firms' response strategies. The only thing worse than facing a situation where a violation has occurred, is having to explain to the court or a client why the firm failed to implement known and widely used measures that could have prevented the breach. ILTA

This article was first published in ILTA's March 2010 issue of *Peer to Peer* titled *"Risky Business"* and is reprinted here with permission. For more information about ILTA, visit their website at www.iltanet.org.