

❖ Constructing Unbreakable Ethical Walls

by Kathy Englar of IntApp

Law firms are paying ever-increasing attention to ethical walls and information security. Business drivers such as mergers, rising lateral-hire activity and overall matter-volume growth are creating more conflicts situations where walls can play a role in mitigating risk and securing client waivers. Even outside of conflicts scenarios, clients are increasingly asking harder questions about how firms are locking down sensitive information within their organizations.

In most instances, firm interest in walls is driven by a client request for increased security for their work product. In other cases, a firm experiences a close-call or near-miss event where they discover that an employee who should be walled from client or firm material is able to or has inadvertently accessed it. In others, insurance providers have mandated that firms demonstrate more extensive ethical wall logging and audit capabilities. Finally, some firms view information security as a competitive instrument and seek to exhibit best practices before a judicial or client audience.

To address these scenarios, law firms are embracing best practices that include deploying information security systems to control access to restricted documents and resources, both within document management systems (DMS) and across other key information repositories. This article highlights several key IT and business issues that organizations should evaluate and address to plan and execute successful ethical walls implementations. While by no means does this article address every issue, what follows delves into several key lessons stemming from real-world experiences working with a broad cross-section of law firms with different priorities and technical environments.

Choosing Your Foreperson

As with any architectural venture, building ethical walls requires solid project management. There are several reasons why effective coordination is key to rolling out ethical walls. For one, modifying information security practices means more than simply adding controls that impact DMS administrators. The tools and procedures firms set up to manage ethical walls and confidential matters impact multiple stakeholders. Firms that choose to implement unified security across multiple applications (such as document, records, financial, CRM and time management) need to involve the IT owners and administrators of these systems.

In addition to technical administrators, support staff and end users also need to be taken into account. Whenever law firms want to change attorney “standard operating procedure,” the changes need to be carefully managed and communicated. By paying special attention to IT project fundamentals such as collaboration, communication and

training, firms will greatly enhance their chances for success from the start.

Therefore, in order to develop a comprehensive deployment plan, organizations should identify a clear project owner (or project committee). This individual or group should conduct an assessment, identify the project team members and build an execution plan including milestones and deliverables.

Drawing Up a Blueprint

Building an effective blueprint for ethical walls requires identifying business requirements and assessing the firm’s existing environment and processes. Most firms have an approach to ethical walls already in place. A universal practice is the circulation of a memorandum to attorneys. Or, in the case of confidential matters, it might mean setting up a separate DMS library accessible only to those with the need to know.

When assessing current practices, organizations should first answer these questions:

What matters, information and systems are currently subject to ethical walls?

How are walls defined, and what’s the process for setting up new ones?

How are wall definitions maintained as the composition of practice teams changes?

Is there an aging and review process for walls?

How is security managed for internal support staff or external contract attorneys?

With an understanding of the current landscape, the blueprint should be extended to define target design and practices including:

What is the target process for creating and managing walls?

Where will definitions of security restrictions be sourced and stored? For example, these could be sourced in a conflicts application, a third-party wall application or custom database.

What security enforcement models are required? For example, some situations may call for exclusionary walls which restrict only specific users from accessing specific client matter information. Other scenarios may call for inclusionary modes that prevent all but an explicitly designated list of personnel from accessing particular data.

Besides the DMS, what other applications need to be secured?



Who will define, configure and manage wall definitions (records/conflicts, IT, attorneys themselves)?

How important is it that security tools are self-aware and update security definitions dynamically based on user activity in applications such as DMS or time entry systems?

What expiration policies are required (standard expiration, indefinite lifespan, defined review period)?

Are other changes in place or planned which might affect walls (for example, a DMS upgrade or migration)?

The blueprint process should also take into account the specifics of the firm's DMS architecture including issues that may affect the design of a walls solution such as:

The number and geographic distribution of libraries

Matter organization within the DMS (whether firms are matter-centric or not will have implications for the ways in which security is enforced and managed)

The process for synchronizing user and client matter data among libraries

With target practices in mind, the plan can be extended to identify and involve administrative stakeholders throughout the firm. This starts with key applications such as conflicts/records, DMS and other relevant systems, and extends to include related support staff. These stakeholders should be brought into the process early and participate regularly.

In addition to administrative stakeholders, end user requirements merit significant attention. For example, the firm should create policies for scenarios such as the process of adding a user to a wall definition or how to treat attorney requests to access restricted information.

Selecting a Contractor and Materials

Firms have choices in software tools for managing ethical walls. When evaluating their options, organizations should consider three important factors:

1. Does the technology support the functional requirements defined in the blueprint assessment phase? Questions to address include:
 - a. Can the tool source walls' definitions from the application or system of choice?
 - b. Does the application support the security models required by the firm?
 - c. Does it provide sufficient audit, logging and notification functionality?
 - d. Can it protect information across data repositories beyond the DMS?
 - e. Can walls self-update and extend based on user activity?
2. Does the vendor meet the firm's requirements for solution providers? Questions to consider include:
 - a. Does the vendor have demonstrated expertise in information security management?
 - b. What is the solution provider's reputation in the legal market?
 - c. Can it supply suitable peer references?

3. If the support of external consultants is required for ethical walls assessment, design or implementation, does the vendor have a relationship with a suitable partner?

Breaking Earth, Building and Testing

With the right plan and tools in place, implementing walls and information security can be a very straightforward endeavor. As IT and other stakeholders work to install and configure the walls software, they should pay special attention to testing. In many instances firms may be best served by first deploying walls on a single DMS library or a system used only for training purposes. As part of testing IT should also:

Create multiple types of walls and security restrictions and validate wall protections.

If the firm is using a walls solution that is self-maintaining, confirm that staff activity triggers the appropriate automatic updates.

Similarly, test that local administrators and users are unable to override the centralized security definitions. This can be done by changing security settings at the local application level and confirming that the walls application overrides the error and sends a notification where applicable.

Validate security performance across applications outside of the DMS infrastructure.

Verify that wall logging functionality is tracking desired activity appropriately for auditing purposes.

Training and Finishing Touches

Finally, the system should be rolled out to a broader audience. In doing so, it's important to conduct special outreach to administrative, support and helpdesk functions so they understand how the impending technology and process changes will affect them and what to expect from end users. For example, attorneys subject to security restrictions may contact support staff with requests for access. Support needs to be properly trained to respond to such requests. Similarly, when rolling out ethical walls, all timekeepers should be notified and provided a mechanism for reporting problems or asking questions.

The Dividends of Due Diligence

The above covers some of the most important details firms should consider and address as part of an ethical walls initiative (there are others, of course). With a clear framework in place, organizations should be properly equipped to address them. As with any construction project (metaphorical or otherwise), due diligence and planning are investments that will pay dividends in the form of smooth implementations, fewer surprises and satisfied end users.

About our author :: :: ::

Kathy Englar, Director of Professional Services at IntApp, has managed successful implementations at numerous AmLaw 200 firms. In addition to ethical walls and information security management, Kathy has deep and practical expertise in best practices for streamlining new business intake, new personnel intake and other law firm data and process management initiatives. She can be contacted at Kathy.Englar@intapp.com.