LAW JOURNAL NEWSLETTERS

Accounting and Financial Planning for Law Firms

An ALM Publication

October 2022

Solving the Information Governance Groundhog Day Syndrome

By Nathan Curtis, IGP and Ben Schmidt J.D., IGP, PMP

Security and privacy start with good information governance, and for many firms — trying to get their information governance policy implemented feels a lot like Groundhog Day. Yes, the one with Bill Murray. Let's take a closer look.

Cybersecurity, regulation and compliance, and data privacy remain the top three issues that CLOs rank as most important for their businesses overall, according to the 2022 Exterro/Association of Corporate Counsel Survey. In fact, the importance is increasing YoY.

The high importance given to these three areas aligns with CLOs' expectations that industry-specific regulations and data protection privacy rules will most likely pose the biggest legal challenges to the business. Sixty-six percent anticipate that regulations will cause the biggest legal challenges this year and 55% list data protection rules as a cause for legal concern.

But what about outside counsel? As the trusted guardian and steward of client information, law firms must have security and privacy processes that meet or exceed their clients' needs.

Here's the thing: Security and privacy start with good information governance (IG), and for many firms — trying to get their IG policy implemented feels a lot like Groundhog Day. Yes, the one with Bill Murray. Let's take a closer look.

Information Governance As Groundhog Day

We hear this more often than one would hope: Firm X wants to have an IG policy approved and implemented. It gets enough buy-in from the executive committee and a policy is drafted.

But then something happens. It stalls. The committee, not knowing how to work around the stall, moves on to other projects, time goes on, and eventually the initiative regains attention years later and the firm is right back at square one — and voila, Groundhog Day. Without naming names, there is a common factor that quite often triggers the stall, and it rhymes with "attorneys."

It's not their fault. Firms need to get better about delivering the business case for information governance if they want to get out of the Groundhog Day scenario. In reality, firms without an IG policy in place or without an updated IG policy that reflects hybrid operations are a ticking time bomb, risking mishandling of client information, an unmanaged breach that costs the firm a client, or worse.

Here's the business case to help your firm overcome attorney obstacles and finally get out of the IG Groundhog Day.

Hybrid Operations: Risk and Reward

First thing's first in making the business case — hybrid operations are here to stay for law firms, and hybrid operations increase the risk firms bear in securing client information.

On the flipside of the risk of hybrid operations is the reward. 86% of attorneys across the industry want to keep a hybrid work schedule, which tells us that attorneys are motivated to keep the flexibility of the work model forged in the pandemic. And here, too, IG is the grease that keeps hybrid operations running efficiently and securely — exactly what attorneys want.

Firms should leverage both factors in making the business case for IG.

Sharing of sensitive business information has migrated from conference room white boards and face-to-face conversations to discussions via digital or online collaboration tools and extended email threads.

This swell of digital activity has presented cybercriminals with numerous new openings for social engineering attacks, accounting for a 64% rise in threat volume compared to pre-pandemic levels, according to a global Mimecast Cybersecurity Survey, commissioned in late 2021.

But security isn't just software. Software is merely one component of a broader platform. In reality, security starts with an IG policy that governs the firm's data, so the firm knows what data it has and where. This is a critical piece in safeguarding information at rest — for instance, personally identifiable information requires different treatment, not to mention the effective application of ethical walls.

At its core, information governance is about security, control and optimization of information. That information can be static, in transit or in use. With hybrid operations becoming prevalent, firms need to be concerned with information in transit and in use in new and different ways than previously.

Information in transit is a source of IG consternation. With firms seeking to make information more readily available via digital pathways, sensitive information must traverse those pathways from start to end point in order to be in use by the employee. Thus, firms seek out technologies which allow them to do so. But technology alone isn't enough.

Let's analogize using a railroad and train example. Getting information to an endpoint (the firm employee working remotely) from a start point (the repository) is similar to a train along a railroad. Certain technologies allow the information to traverse the space from start point to endpoint. And your information is the train, or what is contained in the train.

Sound IG policy dictates that you safeguard the start and endpoint, the railroad, the train, and its contents because the whole thing is in play during the transit. If you leave out safeguarding any point, you leave yourself vulnerable. It would be no different than a railroad operator putting locks on the train cars but leaving the station wide open. A robber is potentially going to find a way around your locks and into the station. The smart operator puts security around all of it.

It's fantastic that technologies exist to allow your attorneys to access and utilize information out of the firm's on-premises environment. But if your firm is lacking a sound information governance policy, you are not seeing the full picture. You are leaving yourself open, which could put you on the wrong end of an attack or exploitation of a weakness.

How Much Is the Lack Information Governance Policy Costing Your Firm?

If your firm finds itself on the wrong end of such a circumstance, the costs are both hard and soft. Hard costs are things like the real dollars in liability to which the firm is subjected. These dollars are difficult to pin down as they vary by case, but the bigger the breach, and the bigger the sensitivity of material lost as a result of poor IG, the bigger the dollar figure.

Soft costs are incalculable. Think about the lack of productivity that comes with cleaning this mess up. Or consider the damage to your firm's reputation when word hits the street that information retained by your firm was called into discovery and compromised a client's position in a dispute years after reasonable retention concluded. Your firm will have cost your clients because of an internal inability to push through a sensible IG policy that would have prevented the circumstance from arising. It will be left to the public to decide "why" you were unable to do it, but suffice it to say that the reasons ascribed to the firm's inability will not be flattering. And any post-mortem will uncover the truth: the firm couldn't do it because internal politics and individual preferences got in the way.

We can use off-site storage costs as another example of the hard costs associated with poor IG. Consider a mid-sized firm with 200,000 boxes in storage and which has kicked the can on IG policy development for 10 years and thus achieved no inventory burn-down. After all, the firm is handcuffed — without a formally adopted IG policy, defensible destruction is simply unachievable.

Assuming modest 3% YoY rate increases, and we are seeing storage providers applying double-digit increases given recent economic trends, along with 1% inventory additions based on a typical rate of $0.25 per standard file box, you will spend $7.9MM over the next decade if you allow Groundhog Day to continue. If at the end of the next decade your firm has finally adopted IG policies that allow for defensible destruction, you can expect to pay between $2.0MM and $2.5MM as compared with $1.0MM to $1.5MM at today's rates applied to current inventory levels.

Any way you slice it, the longer you wait to give IG the attention it deserves, the more your firm loses.

Sponsors, Peer Groups and Outside Parties

At firms that have executed this successfully, there emerge common themes: the correct mix of sponsors, peer groups and outside parties. One cannot overestimate the importance of the right executive sponsor. This person must have the influence and "the buck stops here" power required to move the policy forward through the firm and stick with it as objections are raised.

Getting the right mix on a steering committee, however, is nearly as important. The steering committee should set regular meetings on the books where everyone has responsibilities, setting aside enough time to hammer out policy decision points, and carry action items to completion. Group responsibilities are a great way to leverage peer pressure to get things done.

Finally, having an outside party can be an invaluable player in getting an IG policy drafted, approved and implemented. Oftentimes, the firm needs that outside expert, not only to rely on the drafting stage, but to have someone the firm can point to and say, "these folks know the right way to do this and they know what other firms are doing."

Conclusion

Protection of client information is simply fundamental to the reason law firms exist in the first place. Clients are paying attention to how firms are meeting the challenge of hybrid operations and firms have to step up, get out of Groundhog Day syndrome, and meet that challenge.

*****

Nathan Curtis, IGP, a Lean Six Sigma Yellow Belt, brings over 20 years of experience working with law firms in the U.S. and overseas in developing industry-first solutions across Information Governance, Litigation Support, Digital Imaging, and traditional Office Services. As a consultant for Mattern, Nathan is focused on emerging technologies and their application in the legal environment, driving results through Mattern's customized RFP process, and overseeing service, technology and policy implementations. He can be reached at ncurtis@matternassoc.com.

Ben Schmidt, J.D., IGP, PMP, has over seven years of business strategy and support services consulting experience and prior to that eight years as a practicing attorney. As a consultant for Mattern, Ben focuses on outsourcing, offsite records and informational governance. Ben is also a frequent speaker on varied topics within this space. He has been a guest speaker on the Association of Legal Administrators podcast, Legal Management Talk as well various webinars. Ben has also authored articles and white papers Law Journal Newsletters, Law.com, blogs and other legal industry publications. Ben earned his Juris Doctorate from Villanova University and his undergraduate degree from the University of Pennsylvania. Ben holds certifications as an information governance professional (IGP) and project management professional (PMP). He can be reached at bschmidt@matternassoc.com.