General Data Protection Regulation (GDPR) compliance is not an IT exercise. Cyber security represents a huge risk to firms (records breaches increased 556% in 2016, totaling more than 4 billion1) and GDPR is an important regulation which addresses gaps in data security that contribute to this growing, global problem. Enactment of the GDPR is a regulatory shift that will impact firms’ primary work product—information—and how it’s treated. Not a concern for your firm? With a penalty for non-compliance of 4% of your firm’s annual revenue, you need to be.

Because it impacts every aspect of firm operations, GDPR presents a leadership challenge that must be addressed by management boards and executive committees. After all, they will bear the ultimate responsibility for possible penalties. Policies aligning people, process, and technology must be implemented and led from the top down. Crucial to GDPR compliance is data protection practices.

Firms need to start down that path – today – to mitigate risk and minimize the impact. Here’s some practical suggestions that can be implemented right now:

✔️ Create a data map. It’s imperative that firms know where all their data resides – in both physical and electronic formats.

Much as firms want to believe that all their electronic information sits exclusively within their document management system (DMS), that’s just not true – and a management boards would be foolish to believe otherwise.

Documents and data habitually show up in file shares, email messages and attachments, and certainly within the DMS and content repositories such as SharePoint, NetDocuments, iManage, Worldox, or extranets. Sensitive client data also is contained in time entries (such as in Carpe Diem or Intapp Time), bills, and practice management systems (including Elite, Aderant, and Umbria) and must be addressed.

✔️ Update data policies. Firm practices regarding retention and destruction of both physical and electronic content must be harmonized. Policies must specify who can access what content in which systems. Much will be dictated by clients – and under GDPR, firms are obligated to ask; such requirements often are already spelled-out in Outside Counsel Guidelines.

Typical client policies include ones that specify that all matters must be secured to only the practice group, client team, or

1 IBM’s 2017 Threat Intelligence Index

April 27, 2017
even individual matter team; often, clients may demand that access be further limited – or even not limited at all, allowing open (yet audited) access. Because clients own their data that law firms manage, it’s their decision to make – and firms need to have clearly defined policies that address those requirements.

Policies should identify who in the firm will have the authority to delegate access control (usually the firm’s Head of Risk / General Counsel, or specific client or matter partners). To scale this across a firm, partners will need to speak to their clients, offering them a defined set of options, and agree what’s appropriate.

☑ Designate a Data Protection Officer. Note that this is not the same thing as a Chief Information Security Officer – your DPO will probably be a partner.

☑ Implement technology to control access to data. Firms still operating with open access to all content internally or only relying on ad hoc ethical walls to limit matter access are not in compliance. Firms must implement true confidentiality management to meet the GDPR’s “need-to-know access” restrictions. Clients must be given data portability and opt-out choices, and firms will need auditability to quickly generate reports that satisfy clients’ requests.

The “We’ve got time” Fallacy
On May 25, 2018, the GDPR goes into effect. With a little more than a year to go, how many firms truly are ready for these fundamental adjustments? According to recent surveys, odds are good that your firm is not ready; firms have commenced projects, yet:

- The majority ‘definitely are not’ or ‘don’t know’ if they’re prepared for GDPR
- Less than 50% feel confident they’ll be ready when GDPR kicks off in 2018
- Only 9% expect to be fully prepared in time³

If you haven’t yet addressed the few items identified above, with only a little more than a year left to achieve full compliance, you should be concerned. There are no magic light switches within law firms.

GDPR compliance will require a complex re-tooling of law firms’ core operations: people, processes, and technology. These shifts often take multiple years to implement; therefore, to say there is a year left is almost like saying there’s not enough time, even assuming the firm starts today. However, getting started today would certainly help mitigate that risk by demonstrating reasonable efforts to comply – and appropriate confidentiality management technology exists.

Don’t Fall Behind the Pack
Some of the core requirements of GDPR are not new. EU laws from 1995 called for an “appropriate level of security” reflecting the state of the art for protecting personal data. GDPR expands this to cover “data processors” as well, meaning law firms. GDPR is almost unavoidable, even for firms outside the EU. If a firm client does any business with any EU customers, it applies. EU data is enmeshed in most business matters.

Penalty for failure to comply could be a massive fine – up to 4% of your annual revenue. With firms already facing shrinking margins, these financial penalties would play havoc on the bottom line. Worse is the potential long-term damage to a firm’s reputation from a compliance failure – likely on par with the reputational damage caused by the Panama Papers leak.

Regulatory compliance, including GDPR, ranked second on a recent list of issues keeping CLOs up at night.¹ Firms that have already addressed compliance can now claim a clear competitive advantage by demonstrating high security standards and gaining the trust of clients. Firms that have not are at increased risk of losing those clients. Prominent attention from management boards and executive committees can reinforce the importance of adapting firm culture, workflows, and appropriate technology resources to address compliance. Demonstrating information security management, above and beyond compliance, with the same diligence and assertive leadership as other risks that could damage the firm is key.

The take-away? Firm leadership must take immediate action, today: start implementing policies and procedures, and acquire the appropriate technology to support this important initiative.

---