Thomson Reuters MENA Market Insights

Protecting client confidentiality: advice for legal firms considering a move to the cloud

As cyber-attacks grow more frequent and sophisticated, digital security is an issue that affects businesses around the world. However, in the Middle East and North Africa (MENA), organizations seem to be particularly vulnerable to hacks and privacy breaches.[1] According to the *Middle East Information Security Survey 2016* conducted by PwC, companies in the Middle East suffered larger losses due to cyber incidents than those in other regions – with 85% of respondents experiencing cyber-attacks in 2015, compared to the global average of 79%.[2]

The privacy and security of information is a critical consideration in the legal industry, where firms have a duty to protect all data concerning their clients. In fact, this sector can be particularly vulnerable to cybersecurity threats, due to the vast amount of confidential information that law firms handle. Adding to this challenge is the perception that law firms have less stringent security systems in place than their corporate clients, making them a "soft target" for hackers and other cybercriminals that are after valuable corporate data and other digital assets.[3]

The highly publicized Panama Papers leak is an example of how dramatic the consequences of a cybersecurity breach can be, for both a law firm and its clients. In 2015, an anonymous source exfiltrated 11.5 million documents from Panamanian legal and corporate services firm Mossack Fonseca. These papers contained confidential financial and attorney-client information relating to

hundreds of thousands of offshore entities.[4] While investigations into this issue by both regulators and financial institutions are ongoing, the reputations of Mossack Fonseca and the firm's clients – including heads of state and government officials – have been impacted.[5]

This case underscores the importance of protecting confidential client data from hackers, other cybercriminals and even internal security breaches. In a competitive legal environment, firms that don't offer clients peace of mind in this arena could run the risk of losing business.

The regulatory landscape

There is currently a relative scarcity of independent laws governing data protection and privacy in MENA. In many nations, all the current applicable rules or regulations on data privacy form part of other public laws, such as anti-cybercrime laws, labor laws and e-commerce laws, among others. But with more businesses considering a move to the cloud for data storage, the region is expected to progress towards adopting independent legislation on data privacy.

1 zawya.com/mena/en/legal/story/Cybersecurity_in_the_Middle_East_the_legal_view-ZAWYA20170313053948/
2 pwc.com/m1/en/publications/middle-east-information-security-survey-2016.html
3 blogs.thomsonreuters.com/answerson/prepared-law-firms-face-cyber-security-threats/
4 en.wikipedia.org/wiki/Panama_Papers
5 icij.org/blog/2017/03/panama-claims-solid-case-against-mossack-fonseca

In this context – and in anticipation of more specific data protection legislation being implemented across the region – the onus falls on MENA-based organizations to implement their own robust cybersecurity policies in line with international best practice, as well as any current public or sector-specific laws that are relevant.

At the same time, any MENA-based law firms or corporations that do business with European Union citizens will need to be aware of the the EU's new General Data Protection Regulation (GDPR) – and take necessary steps to prepare for it.

GDPR and its impact on the region

Clients, both individual and corporate, expect their personal data to be handled professionally, securely and privately; solely for purposes that they have consented to. These are issues at the heart of the GDPR, which essentially governs how organizations may collect, manage and process their clients' personal information.

The regulation, which comes into force in May 2018, will have significant implications for MENA-based firms that do business with clients based in Europe. Key aspects of GDPR include:

- Stricter rules around consent
- Stronger privacy protections for consumers
- Stringent data security requirements
- Mandatory data breach notifications

One key impact that this law will have on MENA-based firms is in the area of cross-border transactions and data transfers. With GDPR adding complexity to this already risky and complicated field, it's crucial for legal professionals across the region to be familiar with all relevant local data laws, including GDPR if they are handling personal data that belongs to EU citizens.

It's important that all MENA-based firms are aware of their exposure to GDPR compliance risk, as the regulators have been clear that organizations in breach of this regulation could be hit with fines of up to four percent of annual worldwide turnover, or €20 million – whichever happens to be greater.

While GDPR will certainly exert additional compliance pressures on some MENA-based firms, this regulatory development is also expected to have positive consequences, including the impetus to improve data security policies and practices in the region. This is an ideal opportunity for firms to assess and potentially augment their data protection and privacy compliance processes – as well as the information technology resources that power these.

Considering a move to the cloud?

A growing number of law firms in the region are exploring the possibility of moving to cloud storage and software solutions as an alternative to on-premises computing resources. But – in an ever-evolving regulatory environment – data privacy and security concerns can be stumbling blocks in the path toward cloud migration.

In some ways, security concerns are based more on misconceptions than reality. A well-chosen cloud services provider can offer sophisticated privacy and security features that are often more robust than those of on-premises systems. This is because leading cloud providers have the resources to invest in expert staffing, better quality servers and other technical resources that law firms, especially the smaller ones, may not be able to afford.[6]

That said, on-premises solutions do offer their own advantages. Firstly, because these computing resources are owned by the law firm, they can be fully customized to suit unique business needs. Firms also have complete control over their data and can be 100% certain where this information is stored. However, the steep capital outlays required, as well as the ongoing maintenance costs and expense of hiring specialist IT skills in-house, can be prohibitive.

One solution that law firms in the region could consider when exploring their cloud options is a private cloud hosted by a trusted provider and built with the superior security features that the legal environment demands. This hosting approach offers the efficiency of working on the cloud, yet also provides complete control over private data by restricting access to authorized users. The platform is implemented on a cloud-based secure environment, safeguarded by the client's own firewall.

Preparing for cloud adoption

Firms and corporations considering a move to the cloud are advised to streamline and simplify their businesses by using tools to digitalize their matter, case and client workflow management, and handle their client data in a more structured and auditable way.

There are digital platforms available on the market today that streamline contact information, matter management and information delivery, which would be a great first step for firms looking to prepare for cloud adoption. These systems integrate smoothly with multiple software programs and legal knowledge repositories to break down silos between departments and improve the way that data is shared and managed across the organization.

There are also technology solutions that can provide extensive GDPR compliance support, in the form of resources and guidance for cross-border work, including practice notes, standard documents and global guides for multiple jurisdictions. These platforms also offer information on local legislations that law firms and in-house counsel need to utilize if their work is cross-border and if they're planning to use the cloud.

The GDPR is just one new regulatory development that legal professionals need to be prepared for, in order to mitigate compliance risks and avoid the reputational and financial damage that go hand in hand with data privacy and security violations.

6 blogs.thomsonreuters.com/answerson/law-firm-cloud-computing/

Concluding thoughts

Today's law firms need to be fully accountable for protecting their confidential client data. However, they are also required to provide as much value as possible to their hard-won clients in a more cost-conscious and competitive environment. One way to tick all of these boxes is to consider moving to a private cloud model that offers all the benefits of cloud computing resources on a platform that is only accessible by a single firm.

As discussed, firms keen to migrate to this type of platform in order to gain greater control over their data, are advised to first carefully prepare their data, matter management systems and workflows for cloud adoption.

When planning a move to the cloud, it's essential for firms to find information technology resources that provide sophisticated security controls, such as encryption and the ability to restrict and monitor access. Firms will also need to clearly demonstrate their ability to manage and protect personal data, as well as report breach incidents accurately and in a timely manner.

On a more positive note, those legal professionals that are a step ahead stand to make great gains with cross-border work. Naturally, the most expert, trusted and confident cross-border lawyers will be in high demand in the region, which can be a valuable competitive advantage for these professionals and their firms.

Haley O'Brien
Market Development Lead for Legal
at Thomson Reuters MENA

Haley is responsible for the market strategy and overall product portfolio for Thomson Reuters Legal technology and information business across MENA, Cyprus and Malta. She is the lead on engaging, capturing and analyzing deep market insight to deliver tailored products that enable legal professionals from professional services firms, financial institutions, corporates, governments and regulatory bodies to deliver value to their business.

After earning a B.A. (Hons) in business, Haley has spent the last 11 years working for a number of the leading technology and service providers focused on legal in both a managerial capacity and business director function, and has accumulated a wealth of experience supporting legal clients to help them solve strategic and everyday issues. Her knowledge and experience have enabled her to truly understand law firms/departments, their technology, their processes and the challenges they face.

S054037/11-17