UK Legal Tech Trends in 2018

Pessimistic Security, GDPR and Embedded Artificial Intelligence Will be Core Technology Focus Areas for the UK Legal Sector in 2018.

By Roy Russell, CEO of Ascertus Limited

Last year, perhaps more notably than ever before, the leak of the 13.4 million documents that revealed the hidden wealth of the world's richest and the operations of the offshore financial system – dubbed the Paradise Papers – highlighted the cybersecurity vulnerability of law firms. With law firms being an especially attractive target for cyber criminals, their security measures were clearly found wanting – as well as their role in abetting tax avoidance. The jury is still out on the latter, of course.

It's therefore reasonable to assume that the scrutiny on law firms will increase in 2018 – as will the resolve of hackers to penetrate law firms. After all, law firms hold highly sensitive and confidential data that is extremely monetisable. Law firm clients will consequently demand tangible, demonstrable and even evidencable action from legal services providers on how their data is being protected.

> "Undertaking records management will help law firms know exactly what data they hold, in what format and where. Should a security breach occur, the firm will be able to quickly inform the affected parties and the regulators, as demanded by the regulation."

There's merit in pessimistic security

Law firms will make a concerted shift from optimistic to pessimistic security. Contrary to the need for a generally optimistic mindset in business, when it comes to security, there is merit in adopting a cynical and distrustful approach, given the embarrassing and business-crippling data breaches that have become common place today. The NotPetya ransomware attack on DLA Piper is a case in point – this global firm suffered a full day without phones, six days of no email, two weeks without complete access to older emails and documents – not to mention the direct and indirect costs potentially incurred in the regions of millions.

Law firms have historically adopted an optimistic security approach to their data security. Electronic matter files have been visible, if not completely accessible, across all practice areas. Security is only tightened up literally on a case-by-case basis. The problem is that often, "hacks" or losses of data are in fact actioned by firm employees who may have as much time as they like to view, download and even delete whatever information they want. Likewise, a hacker breaking into the system can utilise any employee's user credentials and have access to the majority of the firm's crown jewels.

In addition to traditional preventative security measures such as securing infrastructure, email security management, and intrusion detection; in 2018 firms will have no choice but to segregate content, establish ethical walls and institute governance policies that allow access to information on a "need-to-know" basis. Firms will apply policies based on practice groups, matter types and any other metadata value. This will ensure that only authorised individuals have access to sensitive data – and in the event of credentials being compromised, the impact of the breach will be significantly limited to the account in question.

GDPR will encourage more advanced approaches to data security

With a security breach comes reputational damage, which in real terms is much harder to overcome and its impact is felt well into the future. Come 25 May 2018, when the new GDPR comes into force, the business impact of a data breach of the like of Appleby (i.e. Paradise Papers) will be debilitating for a law firm. Utilising artificial intelligence engine-based tools, firms will be able to go beyond standard security measures such as analysing application logs, network traffic,

endpoint device activity and files downloaded by systems users. These more advanced approaches to data security such as behavioural modelling, machine learning and forensics will be able to build up accurate common usage profiles or fingerprints of all users of the system.

Leveraging historical and contextual information, such technologies will enable firms to evaluate individual behaviour and automatically alert the organisation based on deviations from normal activities. In doing so, they will be able to build up an accurate picture of user behavioural patterns to actively detect untoward activity by analysing their usage habits such as how many emails they typically send, what types of documents do they work on, who they correspond with, which folders they are authorised to access and so on. This is critical to the ability to proactively identify malicious activity in the event of an employee going "rogue" or their user account being compromised with the hacker having access to the system. In either case, this kind of evidencable activity will also play a crucial role in enabling firms to demonstrate genuine intention to comply with GDPR in the unfortunate event of a data breach.

Furthermore, records management will see a resurgence. Undertaking records management will help law firms know exactly what data they hold, in what format and where. Should a security breach occur, the firm will be able to quickly inform the affected parties and the regulators, as demanded by the regulation. Crucially, it will ensure that the law firm doesn't unnecessarily hold information it doesn't need, which in the event of a hack could end up in the hands of criminals. This is one of the key learnings from the Mossack Fonseca data hack (also known as the Panama Papers leak) – the firm was retaining records going back decades and way longer than they needed or should have done.

"Me too" artificial intelligence (AI) products to grow in number

Recently, many large law firms have dabbled with AI technology, with some building their own systems and others deploying separate tools for areas such as contract analysis, information retrieval, analysing court rulings and more. These firms are now finding that it takes much more time and effort than they had originally anticipated to create these bespoke, from the ground up, AI solutions. The question remains whether they will have the appetite, patience and resources to invest in more than their initial requirement? Will they fully leverage these tools and extend them to multiple projects and different applications?

In 2018, whilst pure AI tools may struggle to get past the adoption of the initial application development, AI will become more widespread as vendors of a whole raft of different software solutions including document and email management, case / matter management and legal spend management will "AI enable" their offerings, making the technology's adoption much simpler and par for the course. End users will not necessarily understand or need to know that AI is now "under the bonnet", but they will come to expect that their applications are more automated, make proactive suggestions, provide practical guidance, and automatically complete routine processes for them.

For instance, in M&A situations, the due diligence that needs to be undertaken is a manual process requiring individuals to review and analyse large volumes of data and documents. Already many firms are looking to use AI to improve the process and make it more cost-effective. Technology is available that automatically clusters content into categories, extracts information and presents the output in users' format of choice – a third-party system, spreadsheet or any other software. Not only is the work undertaken in a fraction of the time, AI error is negligible and certainly much much more accurate than humans, allowing lawyers to focus their attention on the more strategic aspects of the M&A.

Similarly, time and billing is another area that is a prime target for AI application, especially with a fixed fee approach fast becoming the norm for high volume work. AI can historically analyse and classify time taken to complete matters for accurate forecasting, resource allocation and profitability management.

Often, there is a time lag between wider industry and legal sector adoption of technologies, but due to the rapid advancements in technology, the changing global commercial landscape, heightened security threats and broader economic uncertainties, in 2018, technology is likely to play the most prominent role yet.

About the author

Roy Russell has over 30 years' experience in consulting, implementing and supporting software technologies within the UK, European and North American legal markets. He founded Ascertus Limited in 2000, a UK-based specialist of document lifecycle technology consulting and software solutions.