THOMSON REUTERS
ELITE™

PROTECTOR OR PROTAGONIST?

LAW FIRM TECHNOLOGY, CYBER SECURITY AND THE MOVE TO CLOUD

the answer company™
THOMSON REUTERS®

EXECUTIVE SUMMARY

The legal services sector has changed enormously in recent years, with law firms across the globe seeking to navigate a complex and radically shifting cyber security landscape. The continuing evolution of cyber risk continues to drive changes across the industry, with law firms being forced to continually re-examine their cyber security strategies and evaluate the effectiveness of their security infrastructure. Against the backdrop of increasing market competition, tightening budgets and the industry's slow but steady move towards cloud technology, the legal IT community is tasked with an increasingly important role.

In order to generate a deeper understanding of how law firms globally are tackling cyber security, Thomson Reuters Elite launched a research project in early 2017 designed to gather key insights from Chief Information Officers and IT Directors at law firms across North America and Europe.

"Effective cyber security is as much a mindset, as it is a specific project or business function", was the opinion given by one respondent, a Chief Information Officer at a large US law firm.

But what is this mindset—and how do law firms cultivate it to ensure their cyber security defences are best in class? What do law firms regard as key elements of robust cyber security readiness? To what extent are typical law firm cyber protections sufficient to defend firms from sophisticated attacks? How are law firms seeking to identify, understand and prepare for new and emergent cyber threats? What role will cloud technology play in helping boost cyber resilience?

In seeking greater insights into these and other questions, Thomson Reuters Elite gathered evidence via a survey of industry professionals and a series of expert interviews. The research revealed number of key findings:

- A majority of firms intend to make greater use of cloud technology inside the next five years. Critically, most think cloud will not undermine cyber security, but would instead help improve it
- Despite this, there remains to some extent a prevailing attitude within the legal IT community that on-site data storage is inherently safer
- Law firms have a moderate degree of confidence in the effectiveness of their current cyber security measures
- Nevertheless, few firms have dedicated cyber security staff and less than two-thirds have cyber incident response plans in place
- The *reputational* damage caused by cyber breach is of equal or greater concern to law firms than the financial, logistical or regulatory impact
- A wide variety of law firm IT systems are seen as particularly vulnerable to cyber attack; equally, there are a number of potential causes of law firm data loss

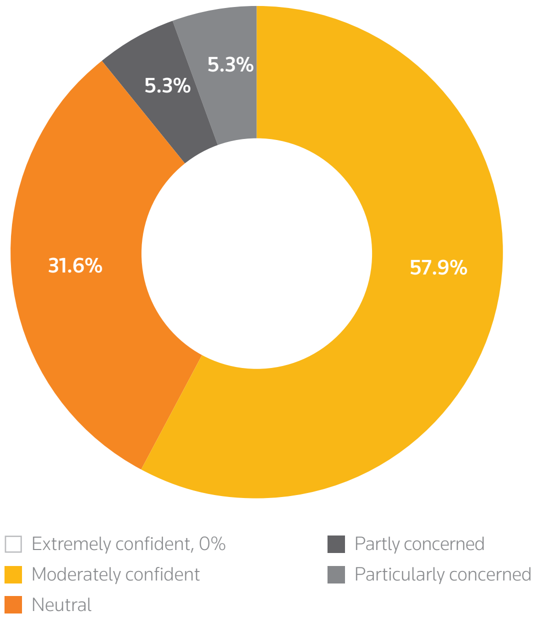
MODERATE CONFIDENCE IN CURRENT PRACTICES, YET CONCERNS PERSIST

Concerns over cybersecurity sit high on the agenda of every legal IT professional. The need for robust security measures grows by the day and, according to one interviewee—a Head of IT at a global law firm—"no-one is confident they are getting it right yet".

Yet despite the complexity of the cyber threat facing law firms, the majority of survey respondents feel 'neutral' (31.6%) or 'moderately confident' (57.9%) in the effectiveness of their firm's existing security measures. One interview respondent had a "relatively high degree of confidence" in existing systems, despite the multiplication of threat factors in recent years.

> *"No-one is confident they are getting it right yet"*
>
> Head of IT, global law firm

Q: HOW CONFIDENT ARE YOU IN THE EFFICACY OF YOUR FIRM'S EXISTING CYBER SECURITY MEASURES OVERALL?



Another interviewee—a Director of IT at a large UK firm—admitted that he was "as confident as one can responsibly be" while admitting there remained a number of things that "keep me awake at night".

"We have stepped up investment significantly in cyber defence over the last 12 to 18 months. Everyone has had to. We are in a much better position than we were, but you can never invest enough".

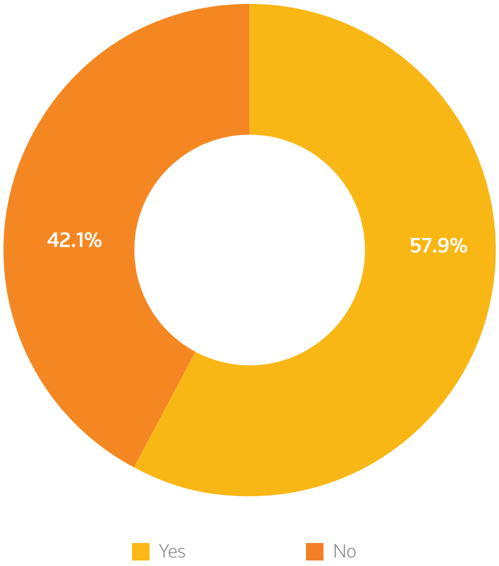
Another interviewee reported his firm had "done a lot of work to improve our preparations because two years ago we just weren't where we needed to be".

> *"We are in a much better position than we were, but you can never invest enough"*
>
> IT Director, UK law firm

Surprisingly, despite widespread awareness of the proliferation of cyber risk, only a little over half of respondents' law firms (57.9%) currently have a cyber incident response plan in place.

Despite this, one interviewee highlighted the importance of robust business continuity planning as an important element of strong cyber security resilience. "You can never be too ready. We focus strongly on scenario planning, particularly around potential ransomware attacks".

Q: DOES YOUR FIRM HAVE A CYBER INCIDENT RESPONSE PLAN?



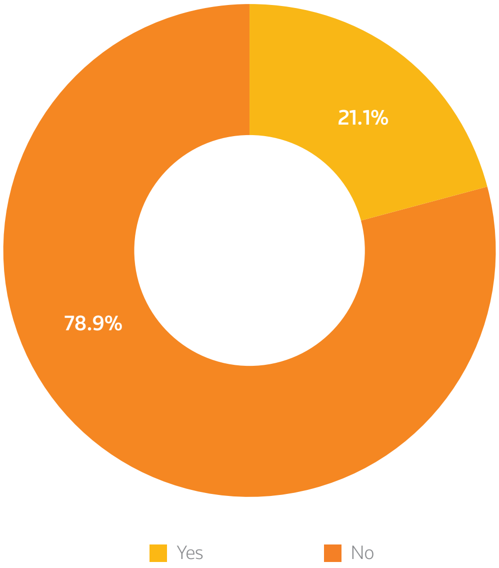
Collaboration internally was raised as an important driver of effective cyber security readiness. One interviewee discussed the "importance of avoiding siloed thinking", and ensuring a sense of "shared responsibility" between General Counsel, risk director and the IT director for ensuring cyber defences are comprehensive and high quality.

"Having data protection lawyers in house is very useful. You need to think holistically as the firm will need not only an effective IT response, but a keen understanding of the legal requirements and also the need for effective communication".

In the UK, the mandatory roles of Compliance Officer for Finance and Administration (COFA) and Compliance Officer for Legal Practice (COLP) were highlighted as particularly important in helping drive this collaboration and internal awareness, engendering an understanding throughout the firm of the risks—and sources of risk—that may affect law firms and their clients.

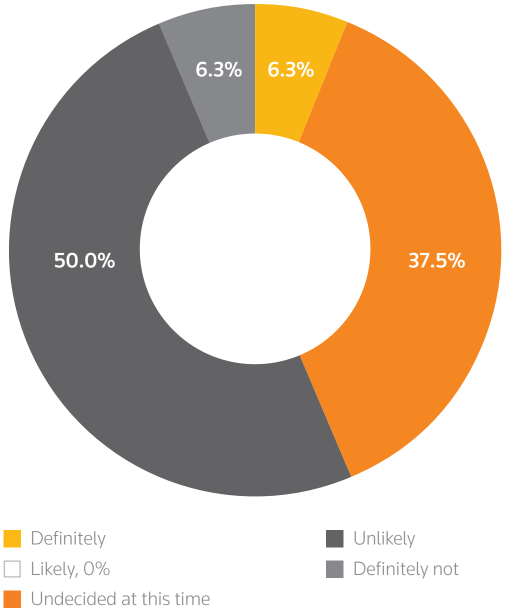
Yet despite this need for collaboration and cross-department thinking, the vast majority (78.9%) of respondents' firms do not currently employ dedicated cyber security staff, of which 50% have no plans to do so in the near future. Organization size was continually identified as the main driver of whether a firm had dedicated staff.

Q: DOES YOUR FIRM CURRENTLY EMPLOY ANY DEDICATED CYBER SECURITY STAFF?



As one interviewee suggested, "You need to be a certain size of firm before you begin to be able to see the ROI" of dedicated cyber security staff. Magic Circle firms have massive cyber security teams. This puts smaller firms at a disadvantage, with smaller IT teams who are typically spread too thinly. Top 30 global firms invariably have dedicated cyber security roles to oversee any issues that arise".

Q: IF YOU DO NOT CURRENTLY EMPLOY ANY DEDICATED CYBER SECURITY STAFF, HOW LIKELY ARE YOU TO DO SO IN THE NEAR FUTURE?



Respondents also highlighted the fact that dedicated cyber security teams not only provide the added resource and capacity to prepare for and handle emergent threats, but also bring a range of specialist security skills that general IT departments cannot match.

UNDERSTANDING THE CYBER RISK LANDSCAPE

Law firms globally are increasingly highlighting concerns about issues such as data residency, protection and the risk of hacking. One interviewee revealed he found that "security protection and compliance needs grow dramatically each year, both in terms of expectations and cost. The risk landscape is changing all the time—and that presents a powerful burden on even a large firm's resources".

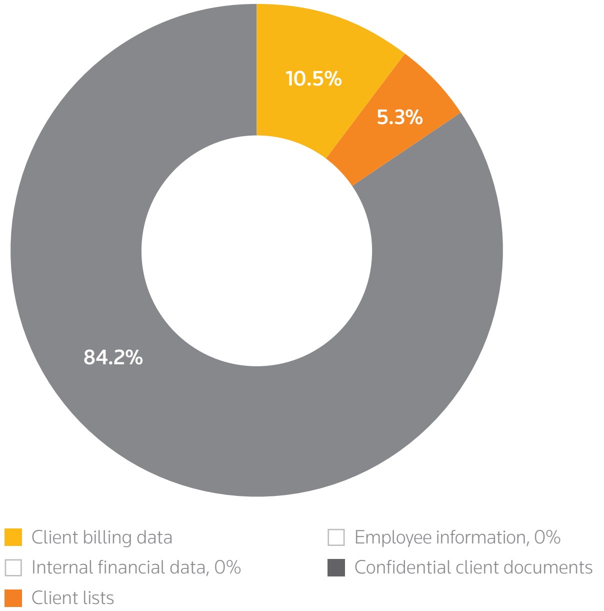
A 2016 study by PwC revealed that cyber attacks on UK law firms rose nearly 20% between 2014-15 and 2015-16, with 73% of the UK top 100 law firms having been targeted in just the last year[1]. In the US, the ABA's 2016 Legal Technology Survey Report highlighted that 25% of US law firms with 500+ attorneys had experienced a cyber attack at some point[2]. However, cybersecurity firm Mandiant suggest the number is higher—that at least 80 of the 100 largest US law firms have been hacked since 2011.

In identifying and evaluating sources of risk, the security of confidential client data was revealed—as expected—to be the greatest concern for 84% of legal IT professionals. Opinion was similarly aligned in judging which IT systems or processes were most vulnerable to breach, with a large majority of respondents (66.7%) highlighting email and other communication channels as the most susceptible point of entry for cyber criminals.

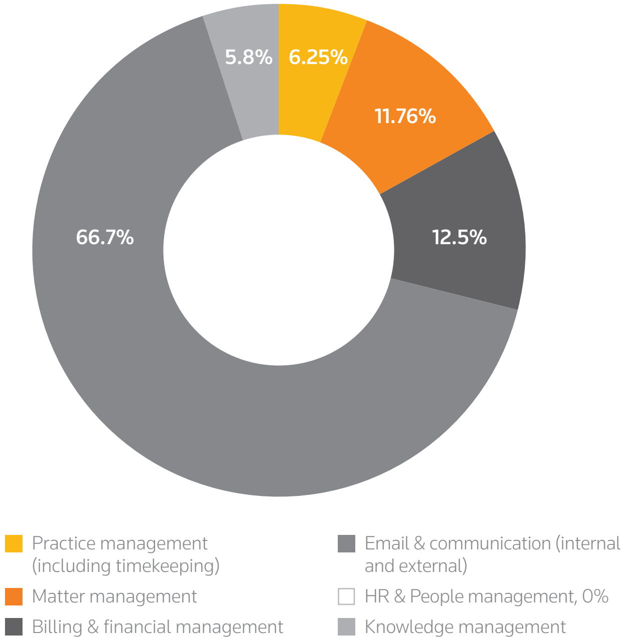
However, opinion was more evenly distributed regarding the most likely cause of law firm data loss, with 44.4% of respondents suggesting malware or phishing, and 33% highlighting human error by an employee.

This was supported by one interviewee, who testified to observing a "massive rise in phishing scams" and "significant threat from whaling", given the "large sums of money being moved around by the firm, meaning it's rich pickings for phishers".

Q: WHAT TYPE OF DATA ARE YOU MOST CONCERNED ABOUT LOSING VIA CYBER BREACH? (I.E. WHAT DATA WOULD BE MOST DAMAGING TO LOSE).



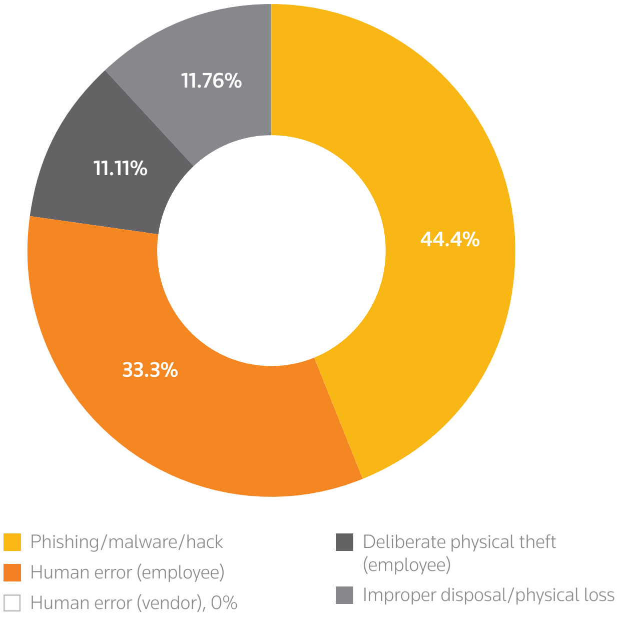
Q: WHAT TYPE OF LAW FIRM IT SYSTEM OR PROCESSES DO YOU THINK IS MOST VULNERABLE TO DATA BREACH?



[1] https://www.pwc.co.uk/industries/business-services/law-firms/survey.html

[2] http://www.americanbar.org/publications/techreport/2016/security.html

Q: WHAT DO YOU CONSIDER TO BE THE MOST LIKELY CAUSE OF LAW FIRM DATA LOSS?



The "mobile nature" of how law firms work was highlighted by one interviewee as a significant risk factor. Law firms typically require IT systems that can be accessed instantly by partners anywhere in the world, ensuring there is a large number of entry points for cyber criminals, driving up the threat risk significantly.

In managing these multiple potential points of entry, a repeated insight was that law firms need to look beyond the technical aspects of their IT's cyber security, and carefully evaluate the risks posed by their own staff members.

One interviewee revealed his firm had deliberately undertaken a significant internal training programme over the last 12 months, not least around staging fake phishing exercises, in order to identify those individual areas of vulnerability and help create better understanding among staff.

> *"Effective cyber security is as much a mindset as it is a specific business function. The challenge is never-ending and you have to keep investing, or you'll be left behind. Cyber security is a lifestyle, not a project"*
>
> Chief Information Officer, large US law firm

Another interviewee commented, "Internal training is important. The best thing is getting people to talk to each other, to help drive education and vigilance internally. Staged exercises also—you need to know who opens what".

With prevention better than cure, the "best cybersecurity measures for cloud should always seek to spot unusual and suspicious behaviour in the interest of data loss prevention. This should even apply to authenticated users".

Indeed, "cybersecurity needs to be inculcated throughout the entire supply chain, from top to bottom", according to one interviewee.

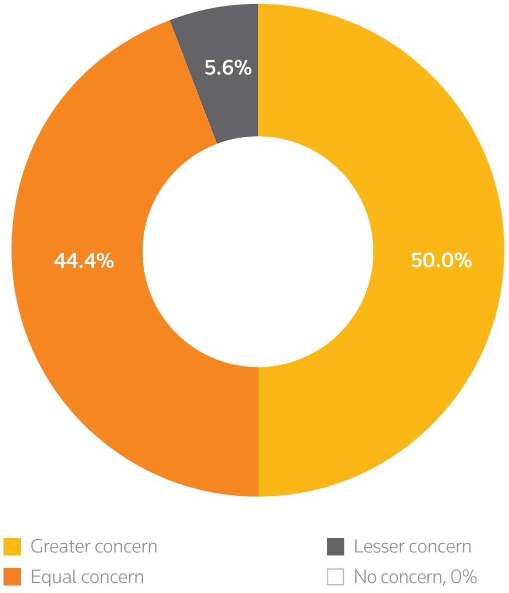
"Human error is the concern, more so than a virus. It's the human factors that keep you awake at night".

According to one respondent, Head of IT at a global law firm, a "major hurdle for the legal sector is its inherent conservatism". Many older lawyers are "change-adverse and prefer the physical over the digital. This can lead to some wilful ignorance" over the risk that cybersecurity can pose.

"Effective cyber security is as much a mindset as it is a business function. The challenge is never-ending and you have to keep investing, or you'll be left behind. Cyber security is a lifestyle, not a project."

Failing to understand this reality risks more than regulatory scrutiny or financial penalty. Nearly 95% of respondents felt that the reputational damage suffered by a law firm following a cyber breach or data loss is of 'greater' or 'equal' concern to the legal, regulatory or financial impact.

Q: TO WHAT EXTENT IS THE REPUTATIONAL DAMAGE CAUSED BY CYBER BREACH AN EQUAL CONCERN TO THE MONETARY, LOGISTICAL OR REGULATORY IMPLICATIONS?



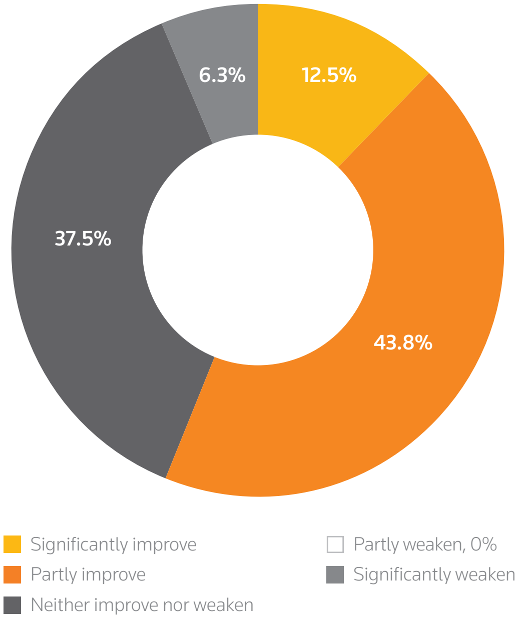
GROWING CONFIDENCE IN CLOUD TECHNOLOGY

In evaluating cloud technology, the primary focus of legal IT teams is naturally the question of data security. The very nature of legal work means that firms are custodians over an immense amount of highly confidential information and the fear of data breach sits firmly in the mind of every Chief Information Security Officer. Pressures to ensure comprehensive data security grow by the day, not least following high profile data breaches covered widely in the media.

In reality, cloud technology presents an enormous opportunity for law firms looking to enhance data security while simultaneously improving enterprise performance and boosting return on IT investment. This was reflected in a number of positive survey responses regarding the security of cloud technology, with 43.8% believing cloud would 'partly improve' their firm's cyber security, and a further 12.5% feeling it would bring 'significant improvements'.

These findings echo sentiments expressed across the market. Recent research conducted by Clutch revealed that 64% of US businesses consider cloud infrastructure to be a more secure alternative to on-premise, legacy systems[3]. Similarly, a 2015 survey by the Cloud Security Alliance revealed 64.9% of IT leaders across sectors believe cloud to be as secure—if not more secure—than on-site servers[4].

Q: TO WHAT EXTENT DO YOU THINK CLOUD TECHNOLOGY WOULD IMPROVE—OR WEAKEN—CYBER SECURITY AT YOUR LAW FIRM?

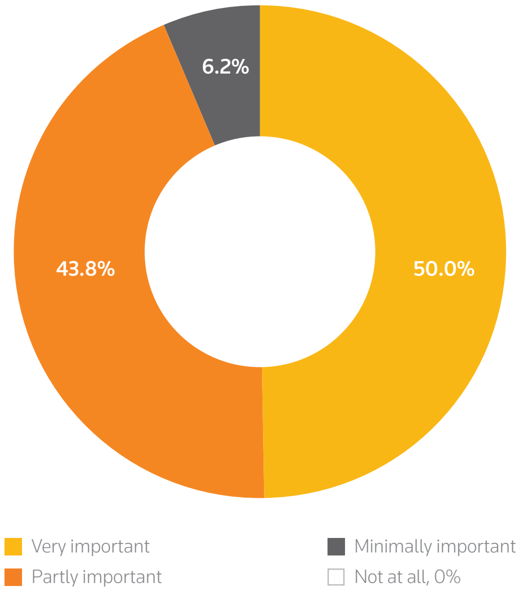


This confidence in the security of cloud technology is further reflected in the fact that more than two-thirds (68.8%) of firms are intending to move more IT systems to the cloud (either for the first time, or as an ongoing process of cloud migration) inside the next five years.

More than two-thirds of firms intend to move more systems to the cloud inside the next five years

In helping provide peace of mind over the security of cloud technology, professional certification (such as ISO, HIPAA, SOC 2 and FISMA) was judged by respondents to be either 'very important' (50.0%) or 'partly important' (43.8%).

Q: HOW IMPORTANT IS PROFESSIONAL CERTIFICATION (FOR EXAMPLE, ISO, HIPAA, SOC 2, FISMA) IN GIVING YOU PEACE OF MIND OVER THE SECURITY LEVEL THAT CLOUD OFFERS?

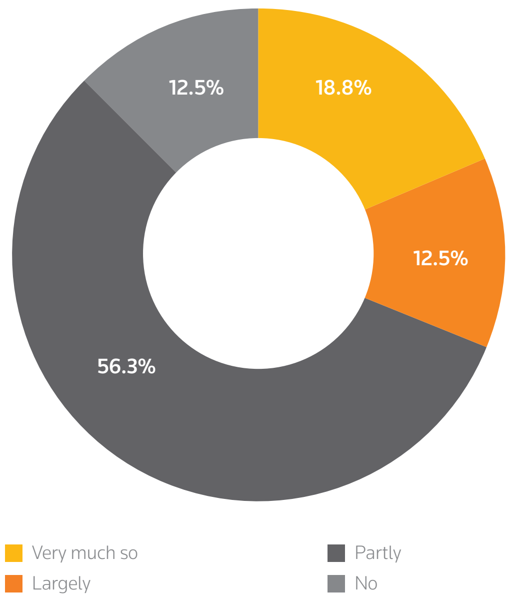


Interestingly, despite industry confidence in the security of cloud technology, an overwhelming majority of respondents believe there is a prevailing attitude within the legal IT community as a whole that on-premise data storage is inherently safer than cloud technology, with more than half feeling this to be at least 'partly' true, and more than 30% believing it to be 'largely' or 'very much' the case.

[3] https://clutch.co/cloud/resources/security-trends-in-enterprise-cloud-computing

[4] https://cloudsecurityalliance.org/media/news/csa-survey-64-9-of-it-trusts-the-cloud-as-much-or-more-than-on-premises-solutions/

Q: DO YOU THINK THERE IS A PREVAILING ATTITUDE WITHIN THE LAW FIRM IT COMMUNITY THAT ON-SITE DATA STORAGE IS INHERENTLY SAFER THAN CLOUD STORAGE?



It should perhaps come as no surprise to learn that some within the legal industry are apprehensive towards cloud. Law firms are inherently risk-averse enterprises, with deeply established methods of working that are typically not easily altered. Against this backdrop, the prospect of moving to the cloud can seem daunting.

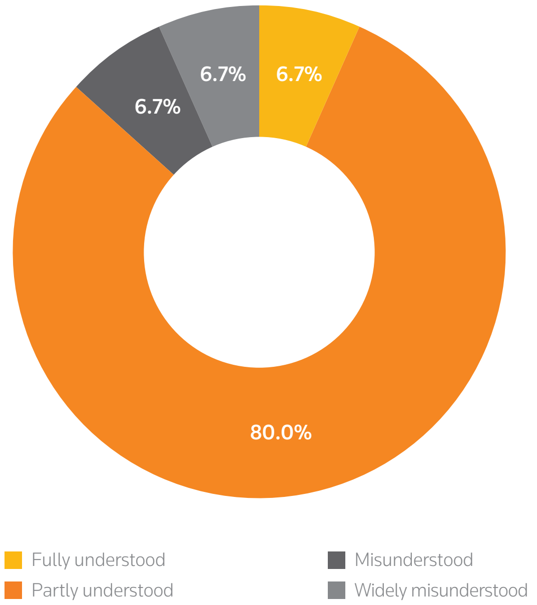
One interviewee, an IT Director at a UK law firm, attested that the "legal industry has forever been something of a laggard in embracing new ways of working". The "realization of cloud technology is still not there. Everyone is talking about it. But not everyone is doing it".

Embracing cloud technology is therefore as much a psychological step for law firms, as it is a strategic or technical one. One interviewee warned the cultural "fear factor" surrounding cloud storage "might always be there" and that many within the legal IT community will always feel more confident if they can "physically see their server – there in the cupboard".

> *"The legal industry has forever been something of a laggard in embracing new ways of working"*
>
> IT Director, UK law firm

This impression was demonstrated further in the fact that a large majority (80%) of survey respondents felt that the strengths of cloud technology (not least its security credentials) are only 'partly understood' by the legal IT community.

Q: TO WHAT EXTENT DO YOU FEEL THAT THE STRENGTHS OF CLOUD TECHNOLOGY (IN PARTICULAR ITS SECURITY) ARE FULLY UNDERSTOOD BY THE LAW FIRM IT COMMUNITY?



Another interviewee, Chief Information Officer at a US law firm, echoed this sentiment, warning of an ongoing "bogeyman fear" within the legal community about cloud technology and its degree of security. Many of these misconceptions are, in his words, "bordering on the silly".

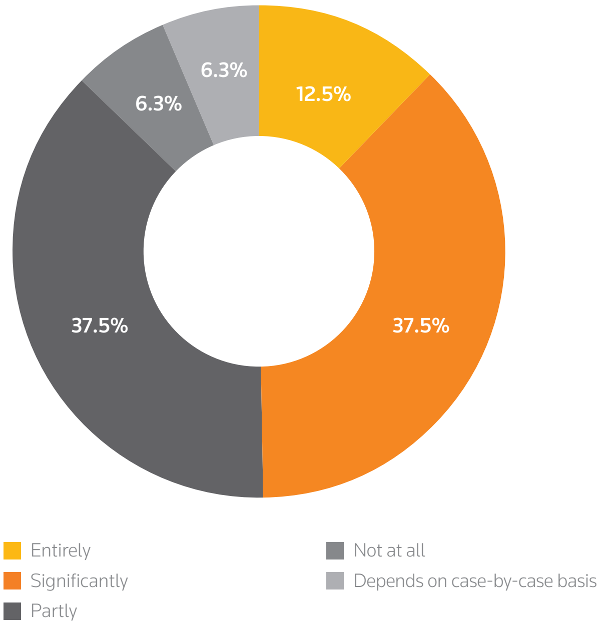
> *"Cloud is a fact of modern life. You have to embrace it, manage it and make it work for you and your clients. You can't just run to the hills and hope it passes by"*
>
> IT Director, UK law firm

One interviewee observed the potential for a generational difference among lawyers in "evolving attitudes towards privacy", believing it will be the "biggest change that will impact the cloud".

"At the moment, it is arguable that the privacy is not really there. Even if this were to improve, we may find younger lawyers, used to sharing their every move on the web, be less concerned about privacy. This does, however, not mean that security concerns will go away – only that there will be more liberality in what is actually ok to share".

Geographical and jurisdictional factors were also revealed to play an important role in driving decision-making around the move towards cloud technology, with 50% of respondents declaring it to be 'partly' or 'significantly' a factor.

Q: TO WHAT EXTENT IS THE GEOGRAPHICAL LOCATION (AND ASSOCIATED JURISDICTIONAL FACTORS) AN INFLUENCING FACTOR IN DECISION MAKING OVER WHETHER TO MOVE TO THE CLOUD?



The stakes are high in legal technology, and it is perhaps to be expected that discussions surrounding the industry's move to cloud technology prompt questions among certain firms.

Against this backdrop, law firms have traditionally felt confident in maintaining their established approach to information storage, utilizing large scale, often highly customized, on-premise servers which can be conveniently managed by in-house teams with finger-tip access.

But this research reveals that attitudes have begun to shift, with growing confidence across the legal IT community and a clear roadmap towards deeper and broader adoption of cloud technology across different law firm systems and processes. According to one interviewee, it's a transition that "might take years, and it's not the case that every firm is ready for it today. However, there's already a strong calling - among medium-sized firms, in particular".

EMBRACING THE CLOUD: BOOSTING SECURITY, PERFORMANCE AND ROI

"Cloud technology offers an important opportunity for law firms looking to boost data security, while simultaneously increasing enterprise performance and return on IT investment. Nevertheless, many within the legal sector remain wary of embracing cloud solutions, often due to key misunderstandings over the reality of contemporary cloud security, which have muddied the debate around cloud technology. Do these misconceptions mean the legal sector risks being left behind?

Instead of viewing it as a security risk, the legal sector should come to see cloud technology as the next generation of cyber resilience, operating full time at the forefront of data security technology, staffed by large teams of specialists well versed in identifying and deploying state of the art data encryption tools and strategies. Cloud providers offer a level of data protection that typical on-site data centers, staffed by relatively small in house teams, can rarely match.

There is a responsibility on technology providers like Elite to help generate greater understanding in the legal marketplace of the cyber security credentials of cloud technology."

Eric Sugden
Chief Technology Officer, Thomson Reuters, Legal Enterprise Solutions

ABOUT THIS REPORT

For this research, Thomson Reuters Elite commissioned an independent research organization—Infinite Global (www.infiniteglobal.com)—to interview and survey a range of senior legal IT professionals from law firms across North America and Europe. A total of 24 survey responses were received, supplemented by three in-depth qualitative interviews from additional firms.

The majority of respondents (62%) came from law firms based in North America. Measured by fee earner headcount, the size of respondents' firms varied significantly, from less than 50, to more than 1000, with a broadly equal distribution in between.

ABOUT THOMSON REUTERS ELITE

Elite is the leading global provider of an end-to-end enterprise business management solution, which allows law firms and professional services organizations to run all operational aspects of their firms, including business development, risk management, client and matter management, and financial management. For more information, visit www.elite.com.