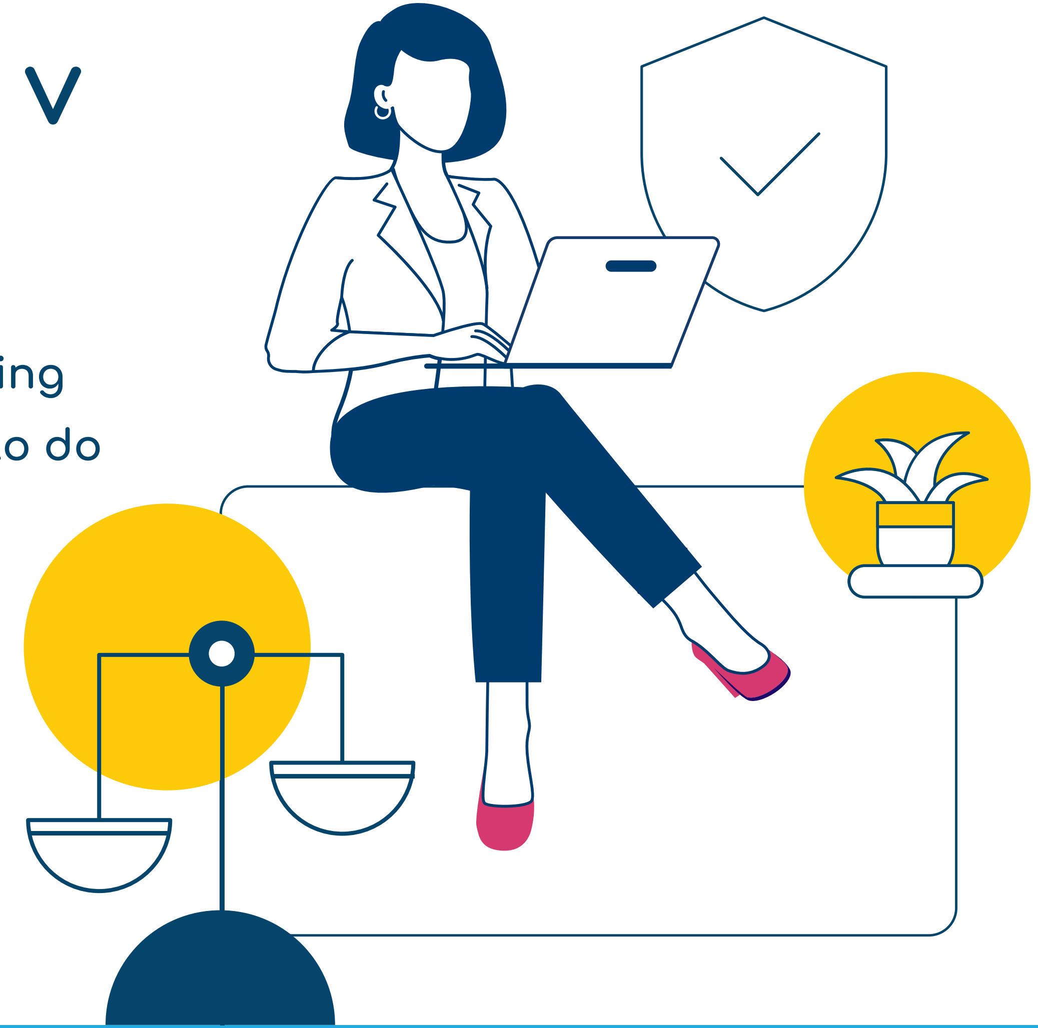
QUILL
A Dye & Durham Solution

Data Accessibility v Data Security

Why accessibility matters, how to avoid growing security risks, and what your law firm needs to do to get the balance right.



Affiliate Partner

The Law Society

There's never been a better time than NOW

Times are changing. The combination of cost- effective broadband, cloud computing, and improved browser-based technologies has facilitated a revolutionary environment where working from home or the office is no longer so different.

This has had a major impact on law firms. In the same way that we no longer walk into our local bank on the high street, we no longer need to travel to our offices to access our practice management systems.

For that reason, data accessibility has never been more important for law firms than it is today. Greater accessibility enables employees to work when and where it suits them, and law firms who recognise this are profiting as a result.

But with greater accessibility comes greater security risks. As you try to empower your employees with flexibility, you might find yourself asking: **"How do I get the balance right between data accessibility and data security?"**

That's what we're here to show you.

In the following pages, you'll discover why delivering accessible data is necessary RIGHT NOW. You'll learn what you need to consider when delivering data on the go and how to manage data using the cloud. But you'll also learn what the security risks are, how they might be addressed and why future trends are important.

By the end, you'll have all the knowledge you need to begin ditching your legacy hardware and to start managing your practice with a cloud-based software like Quill.

At Quill, we've partnered with Google to give our clients the best possible protection against cyber threats. Read on, and discover the secrets for yourself.

Tom Wormald,
Managing Director, Quill

Contents

The death of the 9 to 5

"Tumble out of bed and stumble to the kitchen, pour myself a cup of ambition, and yawn and stretch and try to come to life."

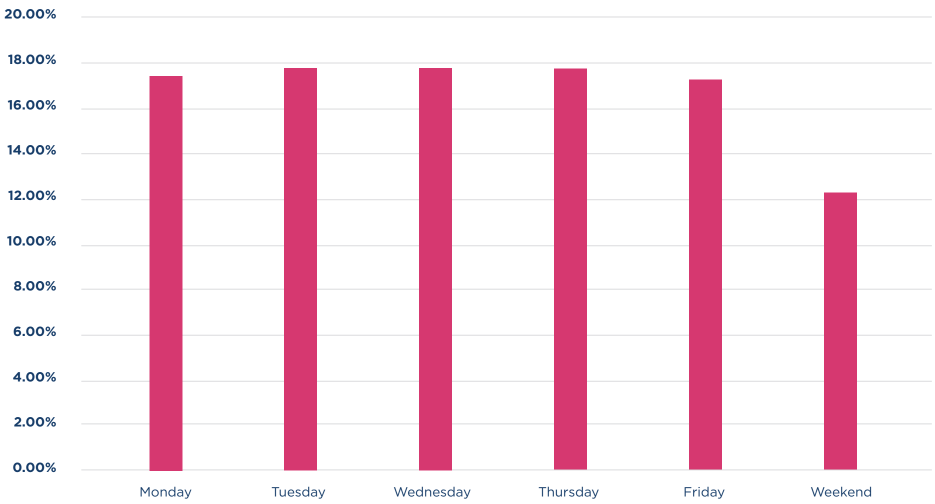
For many law firm employees, Dolly Parton's famous words are a daily reality. But with the advent of newer, more human-centric technologies, people are starting to realise there's a better life out there, and are moving away from traditional ways of working.

So, what does the current working week look like for law firms? We analysed the activity of 10,000+ Quill users, a number representing around **7%** of all law firms across England, Wales and Scotland. Here's what we found...

Getting ready for the weekend

Daily usage data shows us that far more work gets done at weekends than we might initially expect. In fact, weekend activity makes up roughly two thirds of that of an average weekday. That may sound like a lot, but remember that these users now have the flexibility to work from the comfort of their own home, rather than driving into the office on a Saturday morning to clear the decks.

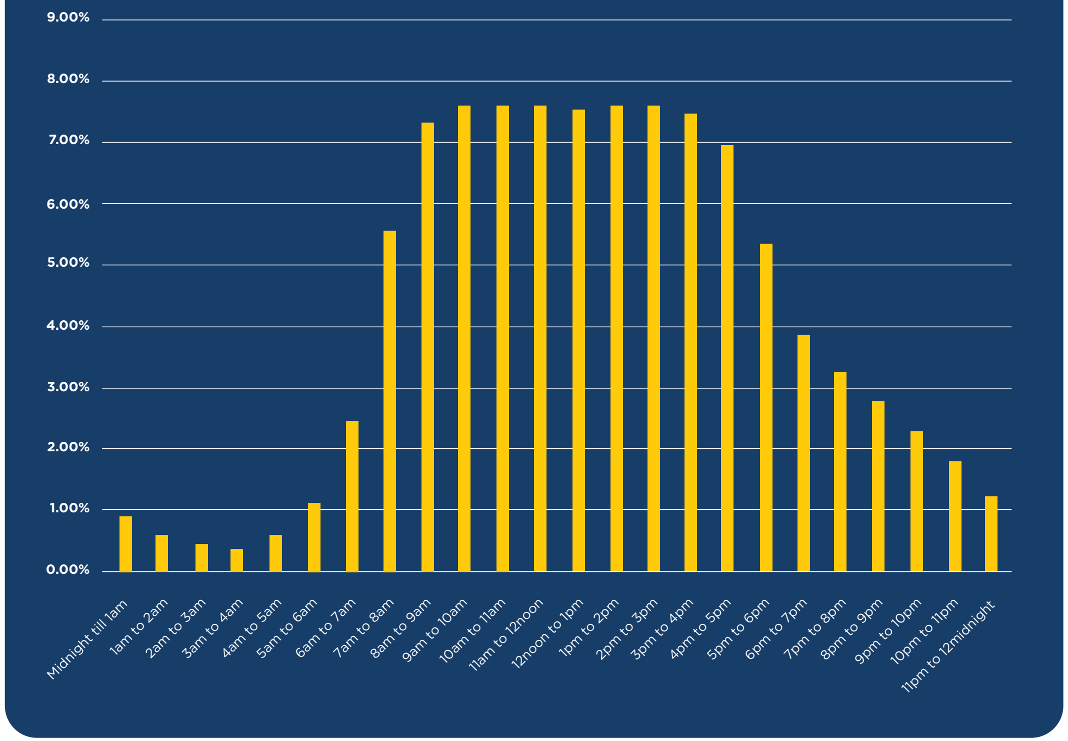
Quill user activity by day of the week



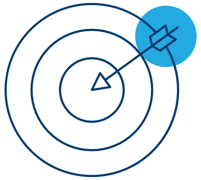
The work never stops

When you look at the cycle of activity on a daily basis, another interesting pattern emerges. There is someone, somewhere, accessing Quill's practice management systems every hour of the day. Whether that's due to preferred working models or whether employees are struggling to complete their tasks within their allocated hours, we don't know. But what's fascinating is that **40%** of all activity by Quill users is outside the traditional 9 to 5.

User activity by hour



With great flexibility comes great responsibility



All this new-found flexibility for your law firm comes with one big problem: security. And if your security isn't completely watertight, then an increase in accessibility will likely be matched by an increase in people trying to access your data illegally.

Why? Because data is the new oil. It's your most valuable asset.

Why you need security

- **To protect your assets.** In the event of an attack, your intellectual property can be compromised. This simply isn't worth the risk.
- **To protect your clients.** If you're at risk, then so is the confidentiality of your clients. Their data is in your hands.
- **To meet legal requirements.** Data protection laws must be followed. Not doing so can cause irreparable reputational damage, even if you don't get attacked.
- **To lower the insurance risk.** The more secure you are, the lower your risk of attack, which in turn means lower insurance costs.
- **To protect your money.** Your law firm could be handling vast sums of money in your office and client accounts, making you a tempting target for criminals.

Enjoy the benefits of access on the go whilst ensuring data security

There can be no successful digital transformation without effective security transformation too. Cyber has become the biggest risk for many law firms and managing it smartly is imperative to long-term profitability.

It's a well-known myth within the legal industry that implementing better security will slow down your digital transformation. But the opposite is true. If you introduce the right security features earlier in the process, then your transformation will be quicker in the long run.

The cost of poor cybersecurity

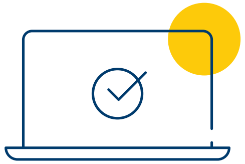
The total amount of data stored in the cloud will reach 100 zettabytes by 2025. That will be **50%** of the world's data at that time.

Source: Cybersecurity Ventures

On average the total cost for a data breach is $4.35 million.

Source: IBM

The old world v the new world



The landscape for defence has changed just as much as it has for attack. Even just 5-10 years ago, the number of malicious groups was relatively small and they were limited to attacking large government institutions. But now, it's completely different. There are a growing number of groups and individuals, all with the time and the technology to target even the most prepared or unsuspecting of law firms.

In the old world, you could afford to take your time when it came to security. In the new world, you can't. You need to act now.

Why act now?

Old world

- Limited number of highly advanced attackers
- Nation-state level resources required
- Targeting governments and critical infrastructure
- Cyber-espionage focus

New World

- Numerous well-funded organisations of attackers
- "Commercial" threat actors
- Broad knowledge of advanced tactics, techniques, and procedures (TTPs), exploits and tooling
- Targeting enterprises of all sizes and sectors
- Financial gain, business disruption focus and data monetisation

Did you know?

In 2020, the World Economic Forum predicted that cybercrime damages could be as high as $6 trillion. That's equivalent to the GDP of the world's third largest economy.

Source: WEF

Improve your security in nine simple steps

Transforming the security of your data doesn't have to be a painful and costly ordeal. By focusing on these nine main areas, you can nullify some of your biggest threats without going drastically over budget.

Physical security

There's still a place for physical security in this digital world. Alarms, locks, shutters and a clean desk policy are your first line of defence against opportunistic intruders. This extends to those working in cafes, courts, trains, police stations, libraries or their homes.

Staff security

Sometimes, the threat is internal. Take care when onboarding new employees to read their references and ensure the right checks have taken place. Check in with remote workers regularly and keep an eye on tailgating in the office — when an unauthorised person slips in behind an authorised user.

Staff licensing

There are certain registration fees your law firm will need to pay throughout the year if you want to adequately protect yourself from money laundering, phishing and data protection breaches.

Staff policies and training

Employees can be your greatest weapon against cybercrime. Everyone in your law firm, from paralegals to partners, should have an understanding of security, and should be aware of any potential security risks that could arise during their work. Build effective training sessions into your induction processes and update them annually.

Passwords

Use passwords for everything. Don't share passwords on email and consider storing them in secure, password management software instead. Better yet, use multi-factor authentication for everything, especially if users can access your data remotely.

Cloud configurations

It's your IT department or specialist partner's job to make sure your routers are configured correctly to ensure certain users can't access things they shouldn't. The same applies to those working from home. Family members should not be able to access your work documents.

Accreditations

It's well worth undergoing the extensive audit process to get your hands on accreditations like Cyber Essentials, ISO 27001 and the Law Society's Lexcel and Conveyancing Quality Scheme standards. You'll notice a whole host of issues which you didn't realise were there and it's a badge of proof that your law firm will do everything in its power to operate securely and protect client data.

Insurance

Professional indemnity insurance and cyber insurance can prevent you from losing a fortune when things go wrong. What's more, having good security protocols in place can reduce premiums, helping you to get cover at a cheaper price.

Third-party protocols

Just because you've got strong security doesn't mean your cloud provider does. Be sure to audit your suppliers and data processors to confirm whether they too are operating securely. If they're not, then you'll be guilty by association.

The data security lifecycle

Data has a long lifecycle. And not a simple, linear one either. It's an amalgamation of smaller lifecycles running in different operating environments. In nearly any phase, data can move in, out of, and between these environments. And it's your job to keep it safe every step of the way.

It isn't simply a case of securing the data at source. You need to be aware of the whole ecosystem of components and protocols that surrounds your data, including your users, your access, your platforms and your applications.

To complicate things further, there's the fact that conflicting laws exist. For example, HMRC can ask to see your data for up to seven years. On the other hand, data protection laws would ask you to delete that data in a lot less time.

So, how do you stay on top of it all? We find the best thing to do is to follow our partner Google's lead, and view the lifecycle in four distinct phases.

The data security lifecycle, according to Google

1. Classify data
Some data is more important than others. The classification stage is simply the process of categorising your data to organise it more efficiently and identify what data needs to be protected. Remember, data can become more valuable over time, which means its classification will need to change accordingly.

2. Apply controls
Based on the classification of your data, you can begin applying controls to protect it. In simple terms, "controls" are just mechanisms you can use to detect, mitigate and prevent cyber threats — think firewalls, data encryption and multi-factor authentication.

3. Monitor
It's important to monitor who exactly has access to your data through a constant process of authentication and authorisation. Not only does this ensure people only access the data they're allowed to, it can also validate the controls you've put in place and detect when people aren't complying with the rules.

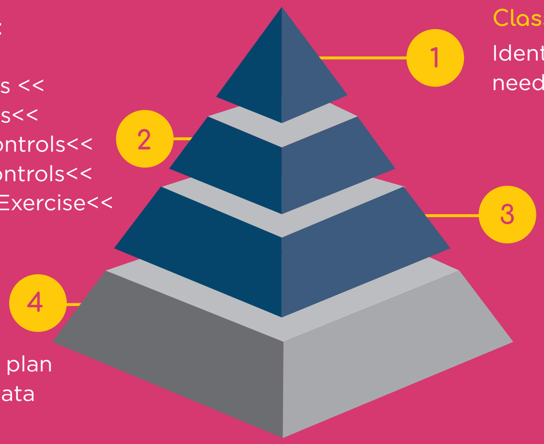
4. Data deletion
A fundamental principle of data security is that any information which isn't necessary for you to conduct business shouldn't be kept. It's a principle known as data minimisation and it helps prevent unnecessary harm. Make sure you understand and plan for the deletion of your data, or simply redact the data if you're unsure.

Data Security Lifestyle

Apply Controls

Protect the data:

Encryption codes <<
Network Controls<<
Authorisation Controls<<
Data Masking Controls<<
Data Reduction Exercise<<



Classify Data

Identify the data that needs to be protected

Monitor

Validate controls and detect non-compliance

Data Deletion

Understand and plan for deletion of data

Source: Shared as part of the 'Get the balance right' webinar, hosted on 16th November 2022 by Quill, Google and The Law Society.

The commercial benefits of cloud computing

There are more benefits to cloud computing than simply improved accessibility. When used correctly, it can bring a number of commercial benefits to your law firm.

Technology is altering the way organisations operate. Now, with the power of cloud computing and AI, law firms are realising they can do so much more with their data. While the security of that data is of vital importance, there's another question which law firms need to consider: "how can we utilise, and get value from, the data we have going forward?"

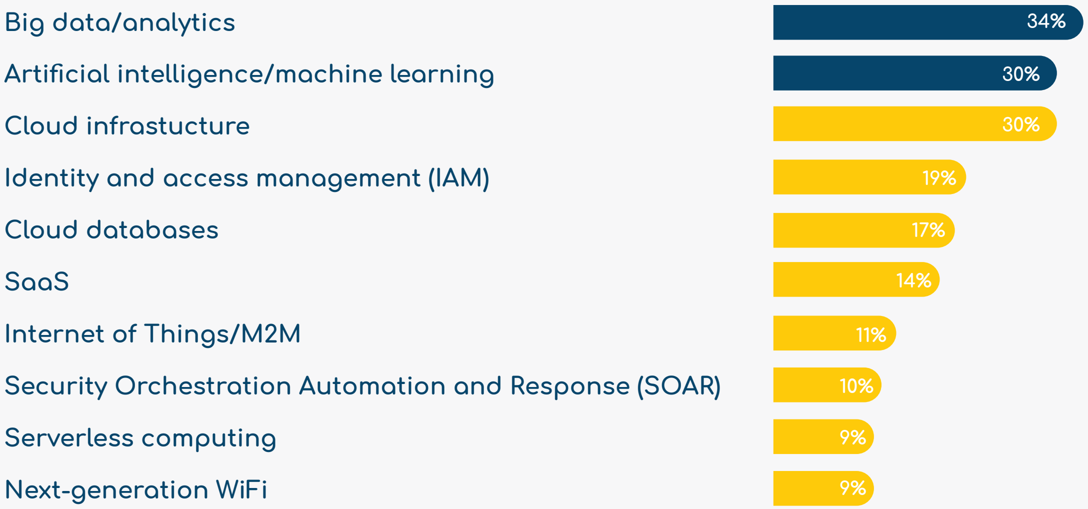
Don't forget the objective

There are inefficiencies in every industry. But in law, the key objective is to serve our clients the best we can. Data enables us to identify exactly what our clients expect from us and where we are falling short.

But while the commercial benefits of this might seem obvious, achieving them isn't so easy. While some **30%** of organisations see the potential of AI and machine learning, just **10%** manage to make significant financial benefits from it.

The problem isn't one of technology, but one of conviction. Moving to the cloud can help your firm clearly identify which areas need to be improved, showing you which capabilities you'll need to add in order to continue delighting your clients.

Organisations see data and AI/ML potential



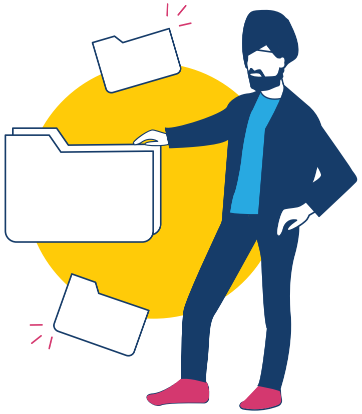
Q: Which of these technologies has the most potential to significantly alter the way your business operates over the next 3 to 5 years? CIO Magazine Oct 2021

But are struggling to make it reality

10% of organisations acheive significant financial benefits from AI

Boston consulting group: Are you making the most of your relationship with AI Oct 2020

The transformation cloud



Cloud transformation is the process of migrating work to the cloud, including data, apps and software programs. Your IT infrastructure can also be migrated to the cloud, if that's in line with your digital transformation objectives.

Now, there are numerous types of clouds for you to choose from online, but perhaps the most important one is what Google calls a "transformation cloud".

A transformation cloud can accelerate your law firm's digital transformation through data democratisation, app and infrastructure modernisation, and trusted transactions. In other words, it allows your team to take advantage of all the benefits which come with cloud computing.

But what is it? Thankfully, it's a lot more simple than it sounds. A transformation cloud is made up of four parts: data cloud, open cloud, trusted cloud and collaboration cloud. Let's look at each of them now.

Data cloud

The data cloud connects all of your law firm's data sources into one unified ecosystem, eliminating silos and making it easier to use your data. It gives you a number of capabilities:

- **Databases:** build interactive global applications that delight users.
- **Data analytics:** analyse all of your data for real-time insights.
- **Business intelligence:** visualise all of your data for operational intelligence.
- **AI:** use the past to predict the future and make better decisions.

Open cloud

The open cloud brings cloud services to different locations, while leaving the operation, governance and evolution of those cloud services to your provider. An open cloud approach enables you to innovate more easily and scale more efficiently — while also reducing technology risk.

Trusted cloud

In simple terms, this is focused on how Google secures its estate in the cloud.

Collaboration cloud

This contains all the utility tools your team needs to work together effectively via the cloud.

A case in point

How Google used data to drive innovation in the law sector

Google was working with a global organisation that was interested in the productivity of its workforce across many different countries.

The firm built a knowledge graph around the connectivity of its lawyers, analysing the way they communicated and connected with each other.

Google Cloud helped surface this data into a dashboard using data-driven techniques. This in turn helped the firm manage and make sure that they had the best people on the right teams at the right time.

The conclusion? Data-driven companies innovate faster.

Four key learnings to finish

At the start of this eBook, we asked the following question: can law firms find the right balance between cloud accessibility and data security? Since then, we've explored the data security lifecycle, changing work behaviours and practical security tips to find out exactly what that balance looks like.

So, what have we learned?

1. Getting the balance right IS possible

We've seen quite clearly that law firms can get the balance right. There's no need to be scared of the cloud. On the contrary, it can offer huge benefits to law firms which are willing to treat it with respect, and take advantage of its improved security functions and protocols.

2. No one can afford a breach

The security threat is getting increasingly costly — to the tune of $4.35 million per breach. Law firms which aren't up to speed with their security already should be looking to change that as soon as possible.

3. Data-driven decision-making is crucial

Basing decisions on data is one of the smartest things a law firm can do. At Quill, we use data to inform many of our business decisions, from what our software looks like, to how it works for our clients. And that's all because data-driven companies innovate faster.

4. Security never sleeps

The challenge of data security doesn't end here. It's a constantly evolving issue that law firms will need to stay on top of if they want to enjoy long-term success. That means training new staff effectively, and ensuring existing employees have their training updated in line with the latest trends and opportunities.

It can take a lot of work, but learning these lessons and putting them into practice is worth the effort. If you can get the balance right, then significant rewards will be there for the taking.

Useful resources

Get more information and give your organisation the best protection possible by following any of the following links.

Get the balance right: free webinar
In this exclusive webinar with experts from Google and hosted by affiliate partners The Law Society, you'll discover the full benefits of a cloud-based software solution and how to identify situations where data security risks could occur.

[Watch webinar]

Get certified with Cyber Tec Security
Cyber Tec Security is an IASME Certification Body committed to improving the security health of businesses across the UK. With their instant quote generator, you can get rapid quotes for Cyber Essentials at the touch of a button.

[Learn more]

Keep your data safe with the ICO
Stay up to date with the latest data protection laws by visiting the ICO's (Information Commissioner's Office) official website.

[Learn more]

Share sensitive information with OneTimeSecret
OneTimeSecret helps people share over 50,000 secrets a month. By using one-time links, it enables you to send sensitive information which only persists for a single viewing, meaning it can't be read by someone else later.

[Learn more]

Guard your organisation against cyber attack with Cyber Essentials
Cyber Essentials is a government-backed scheme that helps protect your organisation from a range of the most common cyber attacks. There are two levels of certification, each of which will give you peace of mind that your defences are in order.

[Learn more]

Make the invisible visible with NCC Group
Just because you don't see the cyber threats and risks, doesn't mean they're not there. As a global expert in cyber security and risk mitigation, NCC Group helps you adapt today, so that you can protect yourselves tomorrow.

[Learn more]

Discover easy, flexible cybersecurity solutions with Duo
Duo helps your organisation, and every user in it, achieve security resilience. Their two-factor authentication, remote access and access control products deploy fast in any environment.

[Learn more]

Be cyber secure with Bob's Business
Bob's Business delivers eLearning solutions that develop and embed a cybersecurity culture within your organisation. Because when cybersecurity training is built to inspire cultural change, it reduces your risk of breaches, empowers your team and promotes responsibility.

[Learn more]

Manage your practice the smart way with Quill
Quill is a one-stop-shop for all your law firm's software and service needs. We take the security of our client's data incredibly seriously, with no compromise on compliance.

[Learn more]

Get the balance right

With Quill's trusted software and outsourced services

QUILL

A Dye & Durham Solution

Quill is an industry-leading legal software and outsourced legal services provider with unrivalled expertise. A one-stop-shop for all things legal, we're proud to be at the heart of over 800 law firms. The first approved Law Society Affiliate Partner to offer outsourced legal cashiering, as well as being able to provide legal accounts, case, document and practice management software, we've been bringing law firms up to speed since 1978.

Affiliate Partner

The Law Society

Contact Quill today E: sales@quill.co.uk T: 0161 236 2910 W: www.quill.co.uk