Hawsons Chartered Accountants
Latest News

April | 2024

Legal Newsletter

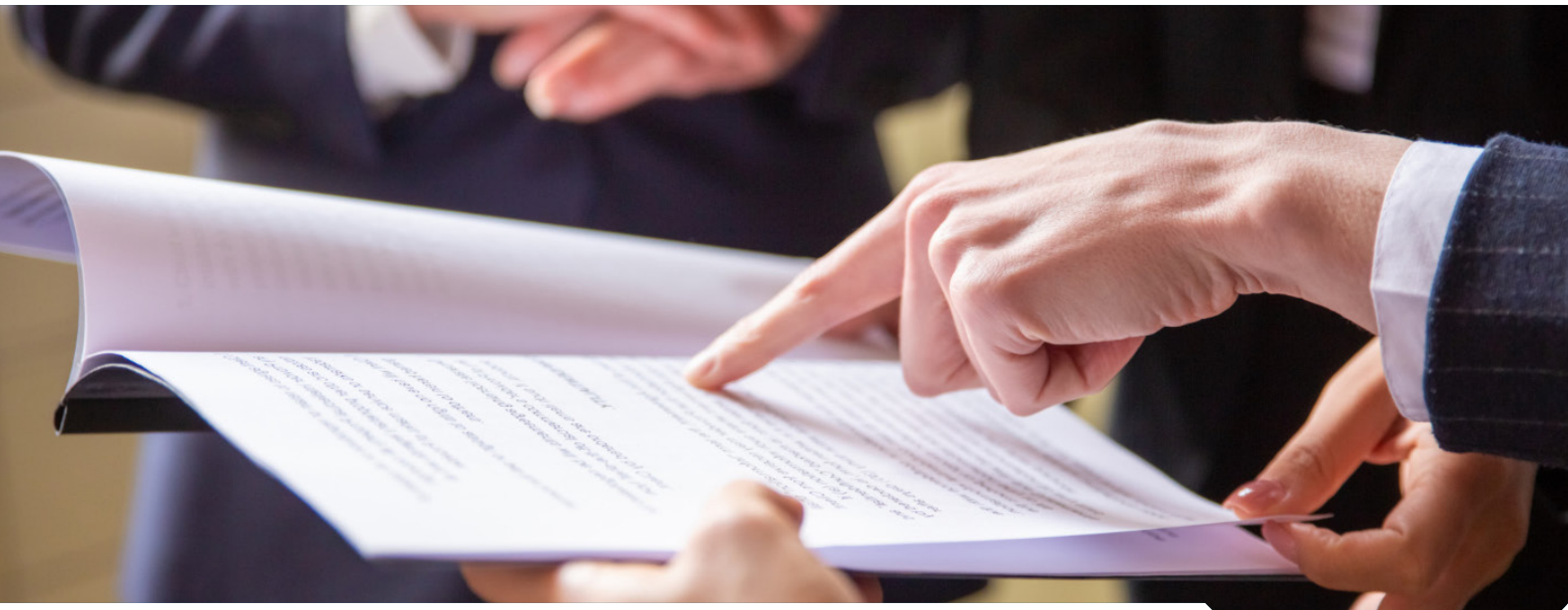
In this issue:

Hawsons

Big firm expertise,
small firm personal attention

Hawsons Chartered Accountants
Latest News

Simon Bladen
Partner



Introduction

Welcome to the latest edition of our legal newsletter. Since our last edition the UK's economy has recovered from a technical reccession at the end of 2023 and the government announced their Spring 'Budget for Long Term Growth'.

In this newsletter we discuss the following topics:

- Sir Geoffrey Vos believes AI will change principles and practices of common law
- Top law firm accounting tips
- Is succession in law firms still a very real problem?
- 2024 ransomware trends

As always we hope you enjoy this newsletter and please do get in touch if you would like more information on any of these articles.

Simon Bladen
Partner

Sir Geoffrey Vos believes AI will change principles and practices of common law

Artificial intelligence (AI) is poised to revolutionise the practice of law, potentially reshaping the principles of common law, according to Sir Geoffrey Vos, the Master of the Rolls. Speaking at the Manchester Law Society, Sir Geoffrey offered an optimistic view of AI's impact, suggesting it could influence various legal specialisms, including company law, insolvency law, contract law, tort law, and even criminal law.

Practical advantages of AI

Sir Geoffrey emphasised the practical advantages of AI in legal practice, suggesting that lawyers may find it difficult to demonstrate reasonable skill and diligence if they fail to utilise these new technological tools. He noted that even the judiciary will face pressure to expedite routine decisions, potentially delegating some tasks to AI systems.

Fears regarding adopting AI

Dispelling fears surrounding AI, Sir Geoffrey likened it to any other tool, highlighting its ubiquity in daily life, such as in smartphones. He argued that concerns about misuse of AI parallel those of any other technological innovation, emphasising the need for responsible implementation.

AI a time saving intervention

Drawing from his own experiments with AI products like ChatGPT, Google Gemini, and Microsoft CoPilot, Sir Geoffrey praised AI's efficacy in drafting contracts. While acknowledging the need for human oversight, he lauded AI's ability to significantly reduce the time required for contract drafting compared to traditional methods.

Addressing concerns about AI's accuracy in legal contexts, Sir Geoffrey suggested that specialised AI systems trained on legal data could outperform generic models. He envisioned a future where AI-generated contracts could become commonplace, compelling clients to opt for cost-effective AI solutions over traditional legal services.

Continued overleaf

Sir Geoffrey Vos believes AI will change principles and practices of common law (Continued)

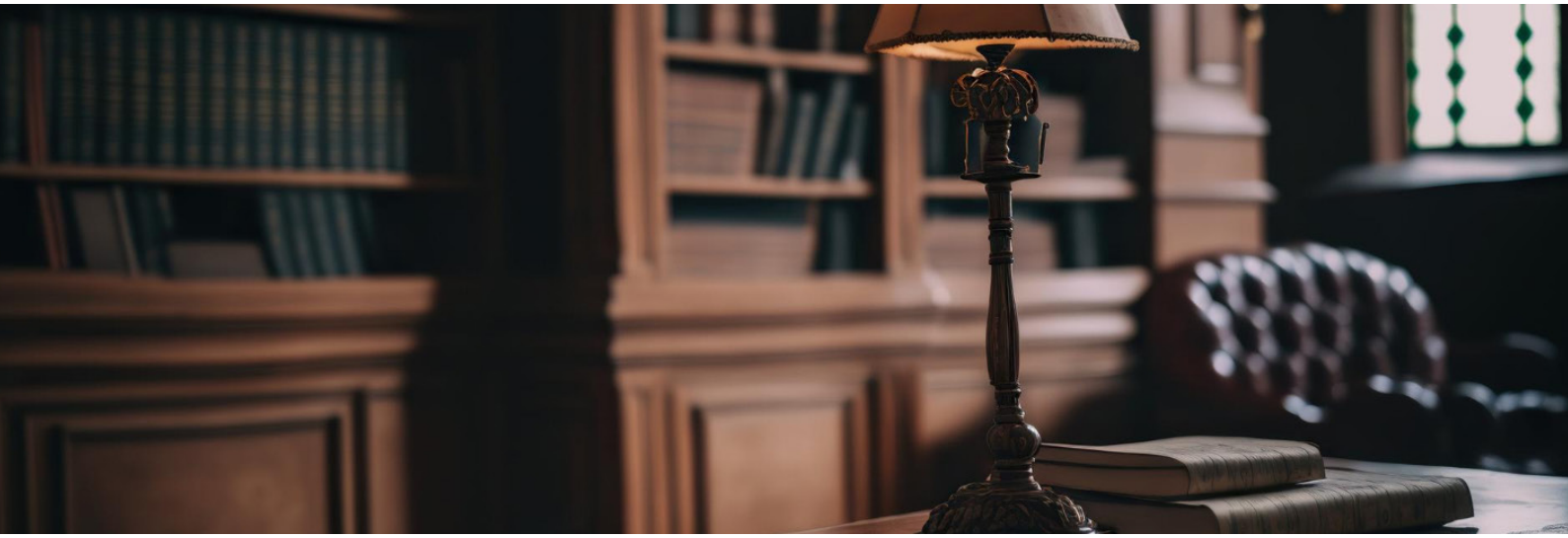
AI's impact on common law and practice

Furthermore, Sir Geoffrey highlighted AI's potential to impact fundamental principles of common law, such as the implication of terms and regulations governing unfair contract terms. He suggested that the nature of the duty of care may necessitate re-evaluation in light of AI advancements.

Regarding the judiciary, Sir Geoffrey noted the receptiveness of senior judges to AI tools, evident in the issuance of judicial AI guidance. He envisioned AI integration within a digital justice system, offering quicker and more efficient dispute resolution methods.

Conclusion

In conclusion, Sir Geoffrey Vos advocated for embracing AI's potential to transform legal practice while acknowledging the need for responsible implementation and adaptation of legal frameworks. As AI continues to evolve, it promises to reshape not only legal processes but also the foundational principles of common law.



Top Law Firm Accounting Tips

Accounting is a fundamental pillar of financially measuring a successful law firm. Law firms, have unique financial considerations that require careful attention to ensure compliance with regulations and business performance. From managing client funds to handling operational expenses, implementing the best accounting practices is essential for helping maintain integrity, transparency and financial stability. In this article, we look into some of the key strategies that law firms can adopt to help streamline their accounting processes.

Separate Client Accounts

One of the foundation principles in law firm accounting is the segregation of client funds from the firm's operational finances (business bank accounts). Law firms often handle large sums of money on behalf of their clients, including fees, disbursements, and settlements. Establishing dedicated client bank accounts ensures that these funds are kept separate from the firm's funds, thus safeguarding against misuse or misappropriation.

Moreover, maintaining clear records of client transactions is essential for compliance with the Solicitors Regulation Authority (SRA) Accounts Rules. These rules dictate strict guidelines for handling client money, including requirements for record-keeping, reconciliations and regular reporting.

Adherence to SRA guidelines

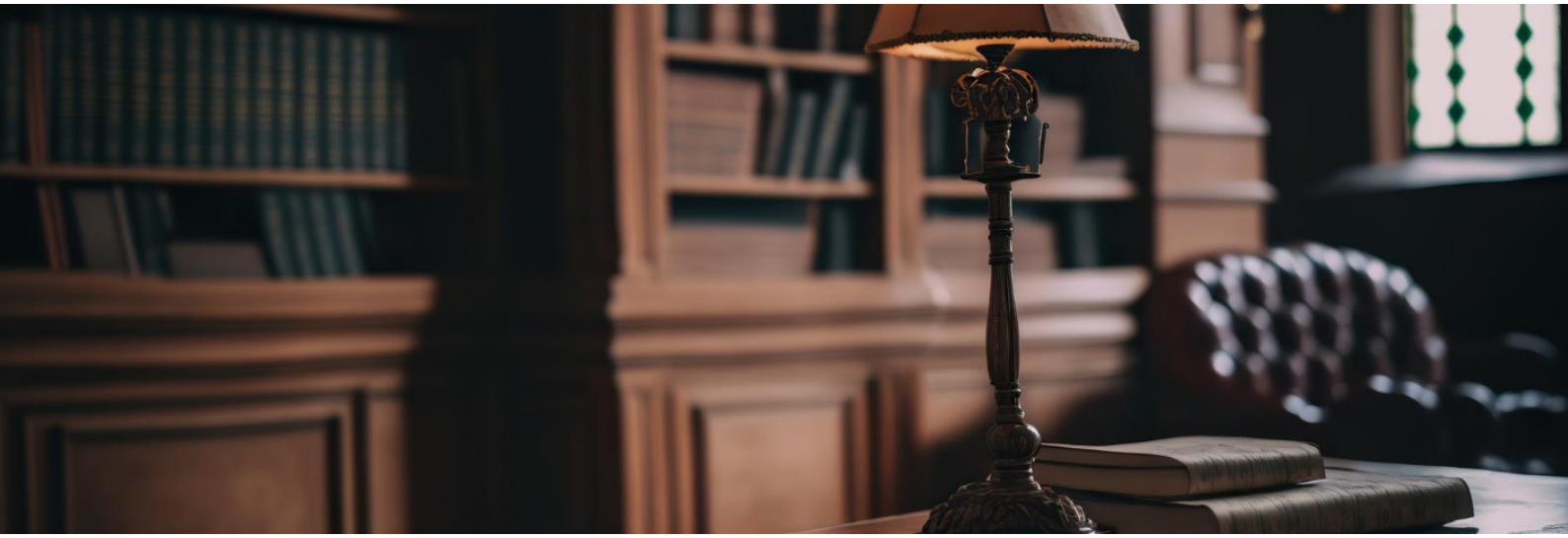
Law firms in the UK must adhere to the stringent guidelines set by the SRA. A strong understanding of the SRA Accounts Rules is imperative for ensuring compliance and avoiding penalties or disciplinary action. Regular updates and training on regulatory changes can help law firms stay abreast of evolving requirements and maintain adherence to best practice.

Accrual Accounting for Revenue Recognition

Accurate revenue recognition is vital for gauging the financial health of a law firm. While cash accounting may seem straightforward, accrual accounting provides a more accurate depiction of a firm's financial performance by recognising revenue when it is earned, rather than when it is received. This method aligns revenue recognition with the delivery of legal services, providing a comprehensive view of the firm's profitability.

Efficient Time and Expense Tracking

Effective time and expense tracking are essential for billing accuracy and maximising billing opportunities. Utilising dedicated software solutions can streamline the process, allowing law firms to record billable hours, track expenses and generate invoices efficiently. Automation can significantly reduce the administrative burden associated with manual timekeeping, enabling law firms to focus their time and energy on delivering exceptional legal services.



Top Law Firm Accounting Tips (Continued)

Budgeting and Financial Planning

Implementing robust budgeting and financial planning processes can help law firms manage cash flow effectively and make informed business decisions. By setting realistic financial goals, monitoring expenses, financial transactions and forecasting revenue, law firms can proactively identify areas for improvement and allocate resources strategically to support growth and sustainability across different departments. Implementing accounting software into your law firm can help you achieve this more effectively and efficiently.

Regular Financial Reviews

Regular financial reviews are essential for assessing the firm's performance, identifying potential issues and implementing corrective measures promptly. Law firms should conduct periodic reviews of financial statements, cash flow projections and key performance indicators to ensure that the firm remains on track to meet its objectives. These reviews also provide valuable insights for optimising operational efficiency and maximising profitability.

Engage Professional Accountants

While law firms possess expertise in the legal domain, seeking assistance from professional accountants can offer valuable support in managing complex financial matters. Experienced accountants with knowledge of the legal sector can provide tailored advice on tax planning, financial reporting and compliance, enabling law firms to navigate regulatory requirements and achieve their financial goals with confidence.

Conclusion

In conclusion, mastering good accounting practices is essential for law firms in the UK to maintain regulatory compliance, foster trust with clients, and measure/quantify business success. By implementing robust accounting processes, separating client funds, adhering to regulatory guidelines and leveraging technology and professional expertise, law firms can effectively manage their finances and position their practices for long-term growth and prosperity.

Is succession in law firms still a very real problem

Succession in law firms is very real problem in the UK The age profile of the legal sector is increasing. The huge wave of legal practitioners who entered the market 30 or 40 years ago are today of an age when they begin to contemplate phasing down or retiring altogether. These individuals have been instrumental in building, marketing and leading the practice in which they work and when they do step-down, they leave large shoes to fill.

In many cases these individuals have large client portfolios with whom they have built a strong relationship over a number of years. That overall contribution to the firm, both financially and strategically, should not be overlooked.

In our experience, transition plans are rarely in place, and where they are, they are often overly ambitious and myopic – failing to give a long enough lead time for successor partners whilst understanding the impact on the firm.

But this is not entirely unexpected given the current economic climate. During covid and the subsequent cost of living crisis firms rightly focussed on short-term decision-making, putting longer-term decisions, such as succession planning, on hold. The result we see today is a potential demographic problem on the horizon.

For a succession plan to be viable, law firms must first buy into it. Practices are full of individuals who are 'top of their class' when it comes to analysis and decision making. But a strong succession plan must be drawn up in such a way that it can be flexible to the developing practice's needs whilst remaining robust.

Key barriers to succession

Some of the key barriers to watch out for when it comes to a viable succession plan are as follows.

Lack of suitable successors: Do the next-in-line have the requisite ambition, skill, and personality to make the step-up?

Upsetting incumbent partners: If partners are approaching retirement age but don't raise the subject themselves, there can become a tendency to ignore the issue to avoid any tension that may result.

Client retention: Clients enjoy stability and value the relationship that has developed over a number of years. By raising the issue of succession we automatically raise the prospect of unwanted change, despite its inevitability.

Looking ahead

Over the next five to ten years many law firms will be transitioning to the next generation.

It is therefore vital that law firms recognise the need for succession planning and determine over what time-frame the issue will arise. In this case, the old adage of 'failing to plan is planning to fail' could never be more accurate.

2024 Ransomware Trends

The cyber security criminals aren't giving up, and they're not just doubling down either. They are now tripling down. They even have virtual "ransomware supermarkets" for criminals to pop in and buy ransomware in a box with a set of instructions so even more criminals can lurk inside your network for weeks on end, planning their attack to maximise the havoc to your business. In this article, we look at some of the ransomware attack trends of 2024.

Current ransomware attack trends that will continue into 2024

In this section, we identify current ransomware attack trends that are expected to continue into 2024.

Supply chain attacks

Supply chain attacks do not just attack a single victim, they usually infiltrate an entire organisation compromising its suppliers or service providers. These attacks exploit the interconnected nature of modern supply chains, leveraging trusted relationships to gain unauthorised access to valuable data and systems. Once inside, attackers deploy ransomware, a type of malicious software that encrypts files or systems, rendering them inaccessible until a ransom is paid. Whilst this is not a new trend these types of ransomware attacks will likely continue. This is because the attackers will usually demand a large ransom because of the types of organisations they target, making it a very lucrative type of ransomware attack.

Triple extortion ransomware attacks

Triple extortion ransomware attacks operate on a three-pronged strategy, combining traditional encryption-based ransomware tactics with additional methods of extortion. The three elements typically include:

- Data encryption
- Data theft
- Reputational damage

In this type of attack, the attackers will seek to infiltrate the victim's network to disrupt operations before stealing sensitive information and demanding huge ransoms knowing that the threat of public exposure could tarnish the reputation of the organisation.

Ransomware as a service (RaaS)

These days, ransomware attackers don't even need to code their ransomware. RaaS is a pay-for-use malware that provides attackers the correct coding to launch and maintain a ransomware attack which now gives more individuals the opportunity to launch a ransomware attack.

Continued overleaf

2024 Ransomware Trends (Continued)

Attacking unpatched systems

Ransomware attacks exploit vulnerabilities in computer systems to infiltrate networks and encrypt critical data, rendering it inaccessible until a ransom is paid. Software companies announce the vulnerabilities they have fixed including the background to what the problem is, and the criminals use that information to set up automated scans across the internet for vulnerabilities.

Phishing attacks continue and are even more sophisticated

Phishing ransomware attacks typically begin with a deceptive email or message designed to lure unsuspecting users into clicking on a malicious link or downloading an infected attachment. Once the victim interacts with the phishing content, an innocent-looking payload is deployed onto their system which can then download the ransomware and set it up without the user knowing anything about it.

After a period of planning, the criminals set the ransomware off encrypting critical files and locking users out of their data. In some cases, ransomware variants may also exfiltrate sensitive information before encryption, providing the criminals with additional leverage to coerce victims into paying a ransom. Whilst this is now a very well-known method of ransomware attack it is still one that is used regularly by attackers and there are no signs of phishing attacks ending.

Ransomware trends for 2024 and beyond

We are now going to explore some new ransomware trends that are expected to evolve into 2024 and beyond.

Attack methods that will evolve to exploit cloud and VPN infrastructure

It is to be expected that ransomware attacks on VPN infrastructure exploitation will become more sophisticated. This will present significant challenges for organisations that use VPNs for remote working and secure communications. The likely attack methods will be on outdated software with security vulnerabilities, weak passwords and multi-factor authentication.

Generative AI could become a huge issue

It is predicted that 2024 will be a huge year for the implementation of AI to help organisations operate more efficiently. However, the rise of generative AI could make it easier for attackers to create more advanced phishing campaigns more efficiently, which means they will be able to target more individuals and organisations with their attacks.

Continued overleaf

2024 Ransomware Trends (Continued)

How to mitigate against ransomware attacks?

1. Employee education and awareness

One of the most critical components of ransomware mitigation is educating employees about the risks of cyber threats, including phishing scams and social engineering tactics commonly used by ransomware operators. Regular training sessions and awareness programs can help employees recognise suspicious emails, links, and attachments, empowering them to take proactive measures to prevent ransomware infections.

2. Implement robust email security measures

Since many ransomware attacks originate from phishing emails, organisations should deploy robust email security solutions to detect and block malicious messages before they reach end-users inboxes. Advanced threat detection mechanisms, such as machine learning algorithms and sender authentication protocols, can help identify and neutralise phishing attempts in real time, reducing the likelihood of successful ransomware infections.

3. Regular Software Patching and Updates

Keeping software and operating systems up to date with the latest security patches and updates is essential for mitigating the risk of ransomware attacks. Vulnerabilities in software applications are often exploited by threat actors to gain unauthorised access to systems, making timely patching updates a critical defense mechanism against ransomware exploits. Organisations should establish robust patch management processes to identify, prioritise, and apply security updates promptly.

4. Implement Access Controls and Privilege Principles

Limiting access to sensitive data and systems through access controls and privilege principles can help prevent unauthorised users from modifying or encrypting critical files in the event of a ransomware attack. By restricting access to only those individuals who require it to perform their job functions, organisations can reduce the attack surface and mitigate the potential impact of ransomware infections.

5. Backup and Disaster Recovery Planning

Implementing robust data backup and disaster recovery mechanisms is essential for mitigating the impact of ransomware attacks. Organisations should regularly back up critical data to offline or cloud-based storage repositories and test their backup restoration procedures to ensure data integrity and availability in the event of an attack. A comprehensive disaster recovery plan should outline the steps to be taken to restore operations and minimise downtime following a ransomware incident.

Continued overleaf

2024 Ransomware Trends (Continued)

6. Network Segmentation and Intrusion Detection

Segmenting networks and implementing intrusion detection systems can help contain the spread of ransomware within an organisation's infrastructure and detect anomalous behaviour indicative of a ransomware attack. By isolating critical systems and monitoring network traffic for signs of malicious activity, organisations can identify and respond to ransomware threats more effectively, minimising the impact on their operations.

Cyber insurance

Even if you've protected your business to the highest level your budget will allow, that protection can still be breached. The mindset has to be one of planning both to prevent the criminals from accessing your network and planning for what happens if they do. Cyber insurance coverage needs to be checked annually to make sure you have the right type and level of coverage so that if your data is exposed your business is protected. As an example, if customer records are exposed, buying identity theft insurance can be very expensive.

Conclusion

To conclude, the ransomware criminals aren't giving up and A.I will only help criminals to work smarter and faster and make phishing attacks more plausible. It doesn't take much imagination to see how criminals could use A.I to take the voice from a YouTube video of your CEO and use that in a social engineering phone call to one of your employees so, if you haven't done it recently, now is the time to review your protection and recovery against ransomware.

Get in touch

Our Legal Experts

Hawsons is one of the few accountancy practices with a dedicated team of solicitor accountants specialising in the needs of solicitors and legal professionals.

We act for a large number of law firms across all three of our offices and offer a wide range of services which are tailored to meet their individual needs. Our legal client base consists of a multitude of firms of varying structure and size, from sole traders to limited companies and LLPs with corporate members.

Our understanding of the unique issues that many in the sector are facing, combined with our technical experience, allows our solicitor specialists to provide you with proactive, commercial and informed accountancy and tax advice.

Simon Bladen
Partner
0114 266 7141
slb@hawsons.co.uk

Sheffield Office
Pegasus House
463A Glossop Road
Sheffield, S10 2QD

David Owens
Partner
01604 645 600
davidowens@hawsons.co.uk

Northampton Office
Jubilee House
32 Duncan Close, Moulton Park
Northampton, NN3 6WL

Dan Wood
Partner
01302 367 262
dw@hawsons.co.uk

Doncaster Office
5 Sidings Court
White Rose Way
Doncaster, DN4 5NU

Hawsons