ISSUE NO.1

VERDICT

A SPECIALIST RISK PUBLICATION FOR THE LEGAL SECTOR

PRODUCT FOCUS

How Legal Indemnity (LI) insurance can help your clients

HOT TOPIC

Digital fraud: the risks blurring the lines between cyber and crime insurance

FEATURE ARTICLE

GDPR and retaining records for Professional Indemnity (PI) claims - a clash of interests?

IS YOUR FIRM CRISIS READY?

Find out our approach to building effective resilience:
ANTICIPATE, PREVENT, RESPOND, RECOVER.

Gallagher
Insurance | Risk Management | Consulting

ABOUT GALLAGHER

Founded by Arthur Gallagher in Chicago in 1927, Gallagher (NYSE: AJG) has grown to become one of the largest insurance brokerage, risk management, and human capital consultant companies in the world. With significant reach internationally, the group employs over 26,000 people and its global network provides services in more than 150 countries.

Gallagher's London divisions offer specialist insurance and risk management services. We provide bespoke policy wordings, programme design and risk placement solutions, and consulting support across a range of specialisms. We manage complex, large, global risks on a direct and wholesale basis and serve as primary access point to Lloyd's of London, London company markets, and international insurance markets.

WE HELP BUSINESSES GO BEYOND THEIR GOALS. IT'S THE GALLAGHER WAY.

CONTENTS

WITH AN INTRODUCTION BY BEN WATERTON

FOREWORD

Welcome to this edition of **VERDICT**, Gallagher's specialist risk publication for the legal sector. While optimism is high amongst UK law firms in respect of business growth over the next twelve months, there is no doubt that regulatory risk is posing a much greater challenge than ever before.

The impact of the EU's new data protection regime, GDPR, has forced law firms to rethink the ways in which they collect, handle, store and secure data. Law firms have always arguably had a higher duty of care for their clients' data, on account of the sensitive and confidential nature of the files and data they keep. Furthermore, the need to retain substantial files and records has long been good business practice for the sector, as a means of helping mitigate the risk of accusations of professional negligence and a need to claim on a Professional Indemnity insurance policy.

Yet coinciding with the introduction of GDPR is a growing challenge: social engineering fraud and more complex forms of data theft. Cyber risks are changing at an unprecedented pace, making it difficult for even the most sophisticated businesses to keep up. However, from 25 May 2018, the consequences for data theft are now more serious. GDPR fines and penalties have the potential to cripple and bankrupt businesses that are found to be lacking in their methods for protecting client data. Those firms that believe their insurance will foot the bill as a result of data breaches or fraud, may be in for a shock, as our article on Digital Fraud reveals.

Increasingly, law firms need to ensure that they are prepared for what in the past would be considered 'low possibility' risks - and be aware of the ever-changing risk landscape. This does not just apply to cyber risks, but also broader crises, such as terrorism and extortion. As such, while the focus right now might be on client data, law firms should be equally mindful of their ongoing duty of care to employees. Our article on Crisis preparedness outlines the right approach to take, in order to protect employees (and your business) from a range of complex risks.

Speaking of employees - since they are a law firm's greatest asset - there should also be a major focus placed on the ongoing attraction and retention of talent. Gallagher's Employee Benefits team have written an article outlining how the key aspects of reward and benefits packages needs to evolve - and how junior talent is now placing greater focus on not just how law firms remunerate staff, but how they support them professionally in their work-life balance. Again, the pressure to deliver a suitable duty of care to employees can be high - and if not managed appropriately, the costs can be significant.

Finally, we outline changing market conditions for Warranties & Indemnities insurance and Legal Indemnity insurance with a range of case studies. These are increasingly some of the most requested policies that Gallagher are receiving new enquiries for - so we outline how these products might support your clients and their businesses.

We hope you enjoy the edition and don't hesitate to get in touch if you want to chat through any of the issues discussed with a Gallagher specialist.

BEN WATERTON
Executive Director
+44 20 3425 3423 | Ben_Waterton@ajg.com

ABOUT GALLAGHER'S LAW PRACTICE

Gallagher, one of the world's largest insurance brokers, provides specialist risk and insurance solutions to professional services firms, and has a track record of working with some of the UK's leading law firms.

We recognise that each industry has nuances when it comes to risk, which means that off-the-shelf insurance products are rarely the right choice. Gallagher organises itself into specialist industry practice groups to ensure that we take a holistic view of risk. We look at risk across all aspects of an industry and then build specific insurance products or risk management solutions around the client in question, from Professional Indemnity and Management Liability, through to Cyber and Crisis Management, Property, Liability, Employee Benefits, and General Insurances. We also help keep our law firm clients up to date with the latest insurance products and trends – helping them keep their own clients one step ahead when it comes to risk.

This means our clients have confidence that their risk profile is properly understood, and that their insurance programme is tailored entirely around their specific needs. Our aim is simple – to provide our law firm clients with specialist insurance solutions backed by great services and support from our experienced team of brokers, risk consultants and claims experts.

01. DIGITAL FRAUD: THE RISKS BLURRING THE LINES BETWEEN CYBER AND CRIME INSURANCE

For an increasing majority of UK law firms – small, large and every firm in between – digital working processes dominate.

Email, networked computers, smartphones and a range of handy apps drive the way we communicate. A variety of web-based order, procurement, financial, banking, HR and other business management platforms now control how we do business.

With such complexity and reliance on technology comes a sophisticated spectrum of electronic threats: from viruses and disruptive malicious software to highly motivated hackers, petty criminals and organised crime. Then there are the acts of careless or disgruntled employees – and even random cyber-saboteurs with no agenda other than scoring cheap and illegal thrills.

The tasty targets for cyber criminals tend to be confidential client information – useful for ID theft – and banking details for straightforward access scams like phishing and robbery by false invoicing. If a client runs an eBusiness for example, a denial of service (DoS) attack that paralyses their website or a 'ransomware' attack that locks systems or information until a release fee is paid can stop their business dead in its tracks. The subsequent damage can be financial, reputational, legal and regulatory in nature – and far-reaching in impact. In addition, changing regulation like GDPR places a even higher duty of care on firms handling personal data. In the event of a breach, fines can be imposed of up to 4% of annual global turnover, or €20m, whichever sum is greater. An investigation into data breaches will take into account how prepared a firm was for a cyber attack and whether the firm took all appropriate measures to secure their clients' data.

Cyber crime - a law firm case study

Type: Server hack and email hijack for invoice fraud.

Scenario: A medium-sized legal practice emailed invoices to nine of its clients, giving bank account settlement details and a standard request to settle payment in 30 days. The practice manager contacted one of the clients after two weeks without any payments and the client confirmed they had settled the invoice immediately on receipt using the banking details given.

Sting: The client sent the firm the payment details and the practice manager checked them against a bank statement. The bank details didn't match and payment had been made to a bogus firm with a similar name. Calling the other clients, the practice manager discovered to her horror that all other eight invoices had been paid using the rogue details.

Investigation: Criminals had hacked the legal practice's server, intercepted the genuine invoice emails and replaced them with the fraudulent versions which they then sent to the firm's clients. By the time the fraud was discovered, the money was already long gone.

Conclusion: Up-to-date anti-virus protection, latest version internet browser and computer operating system may have prevented the fraudulent hack.

Source: Solicitors Regulation Authority (SRA) – Risk/Outlook Report 2016/17/Case Studies – Information & Cyber Crime

Changing risks

The problem with cyber risks is the speed at which they evolve. 'Social engineering' fraud has now become endemic throughout North America and Europe. These incidents are occurring more frequently, the individuals behind them more sophisticated, and the costs to corporations are soaring.

In a typical case of social engineering fraud, information is gathered through the internet or other forms of social media. Fraudsters convince unsuspecting employees to act voluntarily to divulge sensitive information or to perform some task on the fraudster's behalf.

Examples of Social Engineering Fraud:

Mandate Fraud

Employee receives a phone call from an individual who they believe to be a genuine supplier. The fake supplier advises that their bank details have changed and payment is to be made to a new account. Going through procedure, they advise the request must come in writing via email or on company letterhead. The employee later receives an email from what appears to be the supplier, complete with the supplier's signature at the foot of the email. The employee proceeds to change the bank details and payment is issued. Sometime later, the genuine supplier requests payment, indicating that the original payment was never received. Further investigation will identify that the requests were fraudulent.

Fake President Fraud

A mid-level finance employee is the last left in the office one evening. He receives a phone call from an individual who identifies himself as the CEO of the company. He explains that there is a major acquisition about to take place, that the deal must close tonight and that he cannot get a hold of anyone else in the finance team to process the payments.

The employee explains that he only has the remit to transfer funds up to £50,000 and that no-one else in the office to countersign the transfer. The CEO grows more irate with the employee refusing to transfer the funds, repeatedly telling him that he is granting the necessary authority. Eventually the 'CEO' persuades the employee to circumvent the established procedure by issuing multiple £50,000 transfers, totalling £500,000. It is discovered on the next business day that the company has been defrauded.

Falling between the policy cracks

Most companies believe that social engineering fraud would be covered under either a Cyber Liability policy or a Crime insurance policy under the computer/funds transfer fraud extension. However, claims similar to the scenarios above are being denied by insurers. The market argues that neither policy type covers social engineering fraud as standard.

What do my policies cover?

- **Cyber Liability**
  A Cyber Liability policy (often just referred to as 'Cyber') only covers the costs associated with a data breach when third party client data is stolen. Therefore coverage is not triggered with social engineering fraud as no client data is taken. Note it will not cover fines and penalties, such as those that may be result of a data breach following the implementation of the GDPR on 25 May 2018.

- **Crime: Computer fraud**
  If you have the Computer Fraud extension on your Crime policy, the insurer pays the insured for a direct loss of money sustained by the insured resulting from computer fraud committed by a third party. Computer Fraud is defined as the unlawful taking of money resulting from a computer violation. Since in many social engineering cases losses occur as a result of employees being duped into taking action by a third party, the Computer Fraud extension would not be triggered as a third party is not directly controlling or influencing the company's computer systems - the loss follows an internal, not external party, taking action.

- **Crime: Funds Transfer Fraud**
  If you have a Crime policy with a Funds Transfer Fraud extension in place, the insurer pays for direct loss of money sustained by the insured resulting from fraudulently transferred funds committed by a third party. This includes any fraudulent written, electronic, telegraphic, cable, teletype, or telephone instructions, other than forgery, issued by the insured to a financial institution, directing such institution to transfer, pay, or deliver money from the insured's account without the insured's knowledge or consent. Similar to computer fraud, social engineering fraud coverage is not triggered as funds were transferred with the insured's knowledge or consent. With social engineering fraud, the insured had knowledge and gave consent, albeit based on a mistaken basis and therefore the traditional coverages are not triggered.

Most firms are not quite sure where a social engineering fraud loss would be covered. It is often assumed that theft/fraud would be covered by a commercial insurance policy.

Crime or a Cyber policy; it is evident that when it comes to social engineering fraud, not all policies provide the scope of coverage one might immediately presume.

It is also a common misconception within law firms that a PI policy will respond to these losses, but in truth many different factors can influence the response of the PI policy. It is therefore necessary to avoid a silo mentality when considering Cyber and Crime policies; due consideration to the interaction with your PI policy is required.

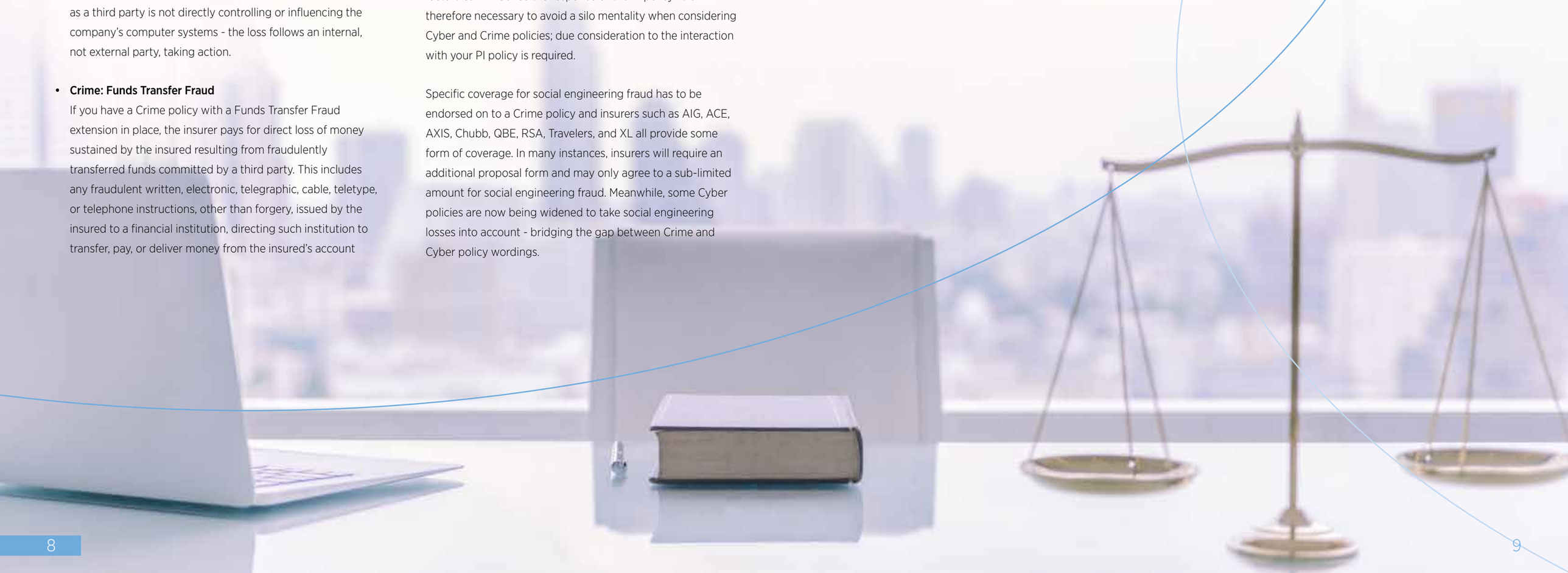
Specific coverage for social engineering fraud has to be endorsed on to a Crime policy and insurers such as AIG, ACE, AXIS, Chubb, QBE, RSA, Travelers, and XL all provide some form of coverage. In many instances, insurers will require an additional proposal form and may only agree to a sub-limited amount for social engineering fraud. Meanwhile, some Cyber policies are now being widened to take social engineering losses into account - bridging the gap between Crime and Cyber policy wordings.

Gallagher's Cyber and Crime teams are at the forefront of these developments. We have specialist Cyber solutions available to help professional services firms manage everything from traditional data hacks, through to more sophisticated fraud risks.

Our policies also come with additional third party support built in, meaning that in the event of an incident, we can help your firm back up and running more quickly.

TO FIND OUT MORE ›

TOM DRAPER
Technology & Cyber Practice Leader
+44 (0)207 204 6223 | Tom_Draper@ajg.com



02.

IS YOUR FIRM CRISIS READY?

As the provision of legal services becomes increasingly global and dependence on digital technology increases, the potential for disruption is rising exponentially. Risks are becoming more complex and more connected.

Threats, such as terrorism, political violence, kidnap and ransom, and cyber risks can cause serious operational disruption, financial loss or adverse publicity that can impact a firm and its profits. That is why it is important to understand crises and the steps firms need to take in order to manage them.

The British Standards Institution (BSI) defines crisis as an "abnormal and unstable situation that threatens the organisation's strategic objectives, reputation or viability" and crisis management as "development and application of the organizational capability to deal with crisis". While your firm may have an incident response plan, incidents are usually something which can be predicted in advance and can be resolved quickly before long-term or permanent impacts occur. Crises, on the other hand, are unique or unforeseen events and can have dire consequences. Failure to respond to a crisis in the correct manner could potentially cripple an organisation and, as this is not something which is part of day-to-day management, companies will need to allocate the time and resource to introduce a crisis management plan.

Research undertaken in 2017 by Gallagher, in conjunction with YouGov, shows that UK companies are keenly aware of the need to build a culture of crisis resilience against the main threats their organisations face, but managing and responding to security threats like cyber extortion, terrorism and emergency repatriation is easier said than done. These incidents are low frequency but high impact – increasingly causing damage to brand and reputation, as well as financial loss and personal injury or loss of life.

The key to a successful crisis management plan is to start as early as possible and have a clear strategic direction including clear communication, effective leadership and a detailed record of all decisions taken. Companies need to shift their mind-set and take a comprehensive approach to building effective resilience aligned to four key pillars of activity: 'Anticipate, Prevent, Respond, Recover'.

ANTICIPATE

The first step in effective crisis management is to creatively consider which threats the organisation may face, and to anticipate those crises in the context of the business. To ensure their resilience, companies should begin by conducting a threat and risk assessment, carried out as part of the analysis stage of standard business continuity planning, and is preferably undertaken with the support of a risk consultant or qualified insurance broker. This process will help an organisation anticipate and understand where its specific vulnerabilities lie. The risk assessment should include multiple components and cover a wide range of potential threat scenarios.

	Physical risk	Digital risk	Human risk	Reputational risk
Definition	Minimising business interruption risk	Minimising data loss or leak	Minimising loss of life or injury	Minimising damage to reputation
Impact on organisation	Denial of access Loss of revenue Costs for recovery/repair	Reputational damage Loss of customers Financial losses	Loss of resource Issues with PTSD	Financial losses Loss of customers
Analysis required	Calculate the impact and likelihood of low frequency, high-impact threats such as business interruption after a terrorist attack	Cyber security audit to determine, for example, the vulnerability of payment and online booking systems and the company's preparedness for a ransomware attack such as WannaCry	Calculate the impact and likelihood of low frequency, high-impact threats such as non-damage business interruption after a terrorist attack	Calculate the impact of a crisis on the brand and reputation, in particular from digital and human risk situations.
Data available to help anticipate threat	External security intelligence companies Social media International and local media Management information from the security team	Management information from the IT department/ CISO Social media Online digital vulnerability databases Cyber security company notifications and alerts	Management information from the HR department External security intelligence companies	Social media International and local media Management information from the communications team of the organisation Public Relations advisors and the press

PREVENT

Building a culture of resilience is an important part of preparedness. Getting it right means more confidence and trust throughout the company and from stakeholders that risks can be prevented or responded to without damage to people, organisational operations and brand reputation.

By taking a comprehensive approach to resilience and putting plans in place that are regularly tested, many companies are able to reduce the total cost of managing risk. Insurance is an important part of the overall picture, but it is a big spend and may not cover the key risks a company might face and only helps with the recovery process, not resilience. By focusing more on anticipating, preventing and responding to risk, insurance can shift from centre stage and become just one part of a true culture of resilience.

Most companies have some kind of insurance cover for threats such as terrorism and ransom, and they can point to business continuity, disaster recovery and crisis management plans. These are all important tools, but they provide a false sense of security if they are not joined up into a comprehensive plan of action.

That means achieving an appropriate balance between identifying, preventing and responding to risks and getting organisations back to normal. Crisis management plans should be short, principle-based and genuinely stress-tested to enable rapid decision-making and communication when there is a vacuum of information, panic and pressure from stakeholders on all sides.

Enterprise Security Risk Management and Enterprise Crisis Management fall within the wider remit of Enterprise Risk Management: like any element of ERM, an escalated approach to the identification, approval and review of risks contributes hugely to disseminating responsibility for crisis, security, continuity and resilience across the organisation. When forming part of an ERM programme, security risks should be presented at senior levels of the organisation alongside the range of other risks that the organisation faces (including health, safety and environment, sustainability, information technology, reputation and brand, and supply chain risk). Integrating the security risk management programme into a wider ERM framework will help the organisation 'compare apples with apples', and will prepare for a range of complex crises in a risk-led way.

RESPOND

Your organisation and people must be empowered with the tools needed to respond in the event of an incident or crisis. Ensure you and your people can respond effectively to any security crisis through training and awareness, coordinated crisis management planning and appropriate insurance cover.

All employees should know their roles and responsibilities should a crisis occur and plans should be tested regularly to help reduce panic. Organisations should take a cross-departmental approach where functions such as risk, HR, security, finance, communications, legal and IT work together to understand, prevent and respond effectively to the broad range of threats and risks that exist. Risks need to be modelled realistically and managed well. Educate your people on how best to recognise and respond in a crisis.

Plans cannot be highly detailed for every possible scenario. Instead the plans should be short, principle-based and stress-tested to enable rapid decision-making and communication at times when there will be a vacuum of information and panic and pressure from stakeholders on all sides. Emergency contacts for insurers, IT providers, and other incident and crisis response experts should be carried by coordinators at all times. Response is also where the value of your people training will become clear. In most cases of terrorism, the 'run, hide, tell' advice of the UK's counter- terrorism police should be followed.

Finally, with regards to cyber risks, every employee with computer access should be trained in the ways of identifying and responding to common cyber-security threats like phishing e-mails and social engineering ploys. The latter seek to obtain access to systems by scamming employees into revealing sensitive information, or clicking on dangerous links to unwittingly download malware. Employees should also know how and who to escalate cyber incidents to within their firm.

Business continuity	Crisis management	Emergency management	Disaster recovery
This type of plan aims to anticipate and reduce the risk of an event before it happens. It is normally made up of a number of different approaches including crisis management plans and insurance. The overall aim is to understand how this can impact your organisation and provide a clear method for dealing with potential threats.	Crisis management plans outline how the organisation will respond in the event of a major crisis such as a terrorist or cyber-attack. These events can have considerable impact on your organisation, stakeholders and the public and if poorly dealt with, can incur significant financial and reputational damage.	Emergency management planning outlines ways to coordinate and manage the first response team should an incident or crisis occur. This includes how to staff an emergency response team including how to assess potential performance, how to plan emergency arrangements and how to train your chosen staff.	This plan takes place after an event occurs and is designed to assess what has happened, how it could be prevented in future and how the organisation can get back on its feet.

RECOVER

When events do happen, a key goal is a swift return to business-as-usual as fast as possible, by use of an effective Business Continuity plan. From a financial perspective, recovery requires the collection of indemnities for insured losses such as business interruption, and the swift repair of systems. A relocation plan may need to be executed. If a crisis elsewhere impacts upon supplies, pre- arranged back-up alternatives should be implemented.

In respect of dealing with business interruption (BI), while many organisations have some form of terrorism or crisis resilience cover in place, they are often unaware that it may not extend to losses from business interruption. This is why it is important to have an insurance policy which specifically protects against non-damage business interruption, where an organisation cannot trade due to an event which is not situated directly on their premises.

Most companies recognise its importance, with our survey indicating that 82% of respondents considered BI to be the most important insurance to have in the event of a terrorist attack. For many organisations, however their BI insurance is inadequate. Property and BI policies generally exclude the risk of terrorism and will not respond if the loss is caused by a terrorist act.

Companies will need to arrange separate cover specifically for terrorism, but calculating the correct sum to insure can be difficult, with many organisations struggling to get this right due to lack of understanding, poor advice, a desire to save premiums and, often, the belief that it will not happen to them. When calculating insurance gross profit figures, risk managers need to give proper consideration to which costs can be excluded. We recommend speaking to Gallagher's specialist Crisis Management team for support on policy structure and coverage advice.

Firms can purchase a Business Interruption policy that insures against loss of profit and increase in cost of working / higher overheads resulting from, for example, fire, storm damage or machinery breakdown. Most Business Interruption policies will include increased cost of operation to provide reimbursement for additional expenditure incurred by you in order to avoid or reduce a reduction in turnover following an insured event. You will need to identify the extra costs that could arise and also determine how long it will take you to get back to business as usual. Finally, you will also need to think about whether all of your customers will return immediately when you get back to normal operation. Losses can seriously disrupt cashflow, and your insurance arrangements will need to provide appropriate protection. Additional cover is available to protect interruption to your business due to supply chain disruption.

Conclusions

Recent events have proved that the world can be a dangerous and unpredictable place. From Las Vegas to Barcelona to Manchester and London, indiscriminate terror attacks are increasingly becoming the norm and new technologies mean that anything including vehicles and homemade explosives can be used to incite terror. No organisation should shelter under the misconception that they are too small or unlikely to be targeted, as many attacks are indiscriminate.

It is a sad reality that these fast-evolving security threats can impact companies of any size, sector or geography and while the greatest risk exposure does come from terrorism, it is actually non-damage business interruption which can wreak the most havoc such as denial of access to premises after being caught inside a large security cordon, loss of trade due to people's nervousness to frequent areas where attacks took place, or unplanned evacuations due to heightened threat levels.

This does not mean that your organisation cannot reduce the risks you face. Companies need to be resilient and adaptable to today's threat environment and while insurance is a key part of this, so is a robust risk management scheme teamed with a culture of resilience. Companies should work to anticipate threats wherever possible and put measures in place to help prevent them occurring. In the event of a crisis you should have a plan to help your employees to safely respond to the threats they face including emergency management and evacuation procedures. Finally, you should have a recovery plan in place to help your firm get back on its feet after a crisis and to help employees recover from any emotional trauma following the event.

In conclusion, a tried and tested risk management plan such as the 'Anticipate, Prevent, Respond and Recover' strategy can help your firm to save lives and ensure that you can respond and safeguard those to whom you owe a duty of care.

TO FIND OUT MORE ›

PAUL BASSETT
Managing Director, Crisis Management
+44 20 3425 3417 | Paul_Bassett@ajg.com

03. GDPR AND RETAINING RECORDS FOR PROFESSIONAL INDEMNITY (PI) CLAIMS - A CLASH OF INTERESTS?

While the implications of the EU's new data protection law, the General Data Protection Regulation (GDPR) for law firms are very broad, in this article, we will focus specifically on compliance with the reforms versus the need to have suitable records to defend negligence claims, and how this might impact the deployment of a PI insurance policy.

At present the GDPR advises that firms ought not to hold onto data for 'longer than necessary'. Unfortunately the 'necessary' threshold will depend on the information, associated legal requirements and other underlying facts; to say that it will be complex and potentially fluid is perhaps an understatement. We will also look at this interaction with other legislation.

Historic Stance

Even before this new legislation a common question posed by many firms over the years was how long should you retain documents before it is reasonable to destroy them?. A good starting point was of course The Limitation Act 1980 and as a consequence most firms adopted the view that files should be kept for at least six years. From our experience (also evidenced in the widely available but specific lawyer's claims triangulations) the vast majority of claims tend to arise within this six year time frame. For lawyers operating in certain work areas there is a likelihood of claims brought under the longstop section of the Limitation Act 1980. Courts will of course consider the 'date of loss' and 'date of knowledge' in deciding when to start the clock ticking on limitation. In some instances, firms took an indefinite retention view in respect of partnership agreements, company formation and trusts. Can this continue?

GDPR vs other legislation

A good example of another file retention conflict is anti-money laundering requirements. According to information from the Law Society, the anti-money laundering (AML) legal supervisors have agreed draft legal sector anti-money laundering guidance taking account of the changes introduced by the Money Laundering Regulations 2017, which came into force on 26 June 2017 (It is marked 'draft' because it is subject to approval by HM Treasury, which is expected later this year, and so may be subject to change).

Included within these requirements is provision to retain customer due diligence records for a five year period after a business relationship ends and/or the date a transaction is completed. However, we suspect that even though this is new guidance, it cannot now be viewed in isolation but must be considered in the context of the GDPR developments. GDPR imposes harsher penalties and transparency requirements, meaning that firms must up their game when it comes to compliance with data protection requirements in the context of AML. One questions how the implementation of combatting money laundering will compare to the need to respect one's privacy; what will take priority and how will policymakers manage this conflict? It is also likely that the GDPR regime will become more onerous over time, forcing companies to manage changing data protection laws where the goal posts are likely to move over time.

The benefits of retaining files in the event of a PI claim

Typically professional indemnity policy wordings are silent on the issue of retention of files. However, you will see claims conditions refer to things like reasonable assistance in cooperating with the defence of any claim, and the use of due diligence to do all things reasonably practicable to avoid or diminish any loss under a policy. Therefore the retention of records can only assist in the defence of an allegation of negligence. From our experience the ability to recall a file (and we have seen the good, the bad and the very ugly of client files over the years) has only ever aided an insured and their insurer in promptly responding to an allegation of loss arising through professional negligence.

Conclusions

How you can protect yourself from the penalties of non-compliance?

Under the previous regime (ICO) fines have been paid by either professional indemnity or cyber insurance policies; this doesn't necessarily mean GDPR fines will be!

In fact, under the new regulations, fines are likely to fall under the category of statutory penalties or criminal sanctions – making them unrecoverable by insurers. These fines are complicated areas, and until they are rolled out it will be impossible to affirm whether they can be recovered under a professional indemnity or cyber policy but you should, at the very least, work with your insurance advisor to ensure the policies wordings have been adapted accordingly.

TO FIND OUT MORE ›

BEN WATERTON
Executive Director
+44 20 3425 3423 | Ben_Waterton@ajg.com

04. THE IMPACT OF GDPR

25 MAY 2018

APPLIES TO:

DATA CONTROLLERS

- Similar responsibilities as under Data Protection Act 2008.
- New obligation to ensure contracts with 3rd party data comply with GDPR.

DATA PROCESSORS

- Legal responsibility in the event of a breach.
- Maintain records of personal data and processing activities.

WIDENS DEFINITIONS OF PERSONAL DATA:

PERSON	LOCATION	WEB ACTIVITY (including IP addresses and cookies)	GENETIC AND BIOMETRIC	ANONYMISED DATA	CHILDREN'S DATA - now has special protections

GDPR PROVIDES INDIVIDUALS WITH GREATER RIGHTS CONCERNING THEIR DATA:

- The right of access
- The right to be informed
- The right to rectification
- The right to erasure / 'to be forgotten'
- The right to object
- The right to data portability
- The right to restrict processing
- The right not to be subjected to automated decision-making including profiling.

GDPR REQUIRES COMPANIES TO:

1. **Abide by the new accountancy principle.** Comply, and demonstrate the firm is compliant.
2. **Maintain records of data processing activities.** These can be requested by the ICO in the event of an investigation.
3. **Ensure consent prior to processing data.** Data should only be used 'where necessary and in the interest of the data subject.'
4. **Secure consent.** Consent is now opt in, rather than opt out. Pre-ticked consent boxes are prohibited. Consent cannot be inferred by silence or inactivity. Firms must inform the data subject that they may withdraw consent.
5. **Update policies and procedures** to manage new rules for subject access requests.
6. **Report breaches.** This is any circumstance where the breach is likely to result in 'a risk to the rights and freedoms of natural persons.' This includes risks of discrimination, reputational damage, financial loss, loss of confidentiality or other economic and social disadvantages.
7. **Appoint a Data Protection Officer.** Required for firms with 250+ employees but recommended for all firms to have an individual accountable for GDPR compliance.

FIND OUT MORE: Ben Waterton, Executive Director +44 20 3425 3423 Ben_Waterton@ajg.com

05. EMPLOYEE TALENT - HOW TO ATTRACT RETAIN THE BEST?

Read this if you are:

› A manager of HR / Reward / Compensation & Benefits in a law firm of 250 or more employees;

› Involved in a merger or acquisition – past, present or future;

› Not 100% confident in your Registered Group Life and/or Excepted Group Life arrangements;

› Unsure whether the firm's benefits meet business and employee needs;

› Under pressure to contain costs;

› Concerned that your Trust Deeds & Rules might be out of date, leaving the firm potentially exposed to uninsured liabilities.

The growing importance of reward packages and employee benefits

UK law firms are confidently reporting strong growth for 2018-19, riding the wave of Brexit uncertainty, as opposed to planning for a storm. With this growth will come the inevitable increase in hiring activity, yet with a shrinking pool of young talent and an increasing employee focus on work/life balance, how can law firms attract - and retain - the best? Firms are also confronting the challenges of an ageing population, namely higher pension contributions and rising benefit costs and complexities. In short, confidence in the ongoing strength, and relevance, of your firm's reward package and employee benefits programme is essential.

Higher expectations

Two thirds of partners of the UK's leading law firms expect their firm's revenue to increase in 2018, according to a recent survey in Legal Week reported on by Zest Recruitment Consultancy. Despite nationwide uncertainty surrounding Brexit and the outlook for the UK economy in general, 49% think the financial outlook for 2018 is better than 2017, and an additional 17% expect it to be significantly better. The survey also revealed that partners expect merger and acquisition (M&A), banking and finance, and dispute resolution, to be the busiest practice areas in the coming year.

Meanwhile, although business confidence is high, commentators predict more M&A activity amongst legal firms themselves, particularly in the UK's small to mid-tier market.

30% of partners expect to see more recruitment in 2018, while 31% of partners also expect US firms to continue their expansion into London and hiring more staff in the next twelve months.

Pay isn't everything

It is widely documented and understood that the proportion of those of a working age in the UK is shrinking, whilst those of a pensionable age is increasing. In the race to hire the best talent from this ever-decreasing pool, it is worth noting that the changing expectations of employees - in a nutshell, pay is no longer the only concern.

A recent survey of legal professionals by specialist recruitment firm Major, Lindsey & Africa found that more than half of respondents would trade in a portion of their compensation for another benefit, with more time off cited by most, followed by a more flexible work schedule and reduced billable hours. When the results of the survey are analysed by size of firm, more respondents from small to medium sized firms (up to 2,000 lawyers) would be willing to trade compensation, than those from larger firms.

Reputation matters

Although salary remains arguably the biggest pull for the current working generation, for the law industry's future talent, pay is now considered alongside the value that prospective employers attach to diversity and inclusion, work-life balance and support for stress and mental health. Today's newly qualified graduates and junior lawyers will be making their career move decisions on these criteria, not just base line salary expectations. Recruitment sites, such as Glassdoor, only increase pressure on firms to concentrate on policies around these aspects of employment contracts.

Transparency in all these areas will increasingly become the norm thanks to a combination of elements:

- **Gender pay reporting.**
  A number of legal firms reported early, revealing significant pay gaps. The underlying causes are numerous but perhaps the most prevalent point is the lack of women holding senior industry positions. Despite the fact that there are more women working in the legal industry than ever before, female legal professionals still only represent 25% of partners in leading UK law firms and just under 19% in Magic Circle firms. Those companies that have reported also include their plans for change, including the establishing of gender equality working groups with input at Board level.

- **Mental health.**
  70% of qualified junior lawyers in the UK report that they are 'regularly' stressed as a result of work and 21% 'occasionally' stressed, according to a Law Society survey. Stigma is still a huge issue in an industry where people are expected to cope with long hours and huge workloads. The Prime Minister last year committed to help reduce the stigma in the UK surrounding mental health, culminating in the government-commissioned independent Stephenson / Farmer Review, highlighting how employers can better support employees, along with the pledge to deliver a national mental health literacy campaign this Autumn. We expect corporate positions on mental health support to become increasingly reported in the press.

- **Corporate governance reform.**
  Whilst the finer details are yet to be ironed out, reform will inevitably necessitate more effective engagement between parties and employees in future. As stated in the government's response to the consultation (August 2017) a new set of principles are being established with the aim of strengthening the voice of employees and other non-shareholder interests. These aspects are highlighted as important components of running a sustainable business.

- **Human capital reporting.**
  There is mounting pressure for firms to report publicly on their approach to employee wellbeing and mental health. The Chartered Institute for Personnel and Development (CIPD) last year called on the government to introduce mandatory human capital reporting standards. Some firms are taking a pre-emptive approach. An article in The Telegraph reports on research by London startup Soma Analytics, which found that FTSE 100 businesses that used the words 'mental health' or 'well-being' more than twice in their annual reports enjoyed a mean profit of £1.4tn, three times that (at £563bn for the year) of those that did not employ such phrases.

Review your offering

Ensuring a competitive reward package and employee benefits strategy that helps attract and retain talent can be a challenge. It must:

- keep pace with employee and business needs
- have a strong governance framework that delivers robust pension scheme management
- ensure that any insured arrangements are both compliant and fit for purpose.

There are plenty of ways to make your reward packages more competitive:

The Lifetime Allowance (LTA):
LTA is due to increase to £1.03m in the 2018/19 tax year and many employers are not being given sufficient information when transferring Registered Schemes to Excepted Group Life policies in respect of how the policy ought to be structured. The firm also needs to consider how much risk it is willing to take and whether to apply the change only to certain individual employee contracts for whom the LTA is most relevant, or all staff.

Gender pay gap reporting:
If the firm has not done so already, consider going the extra mile by the next reporting deadline and extend reporting to the broader diversity and inclusion programme: ethnicity and disability. The Equality and Human Rights Commission made suggestions to this effect recently in its report Fair Opportunities for all: A strategy to reduce pay gaps in Britain.

Pension contribution increases:
The first minimum pension contribution increase recently kicked in. It now stands at 5% (3% employee / 2% employer) and is set to increase to 8% by April 2019. Encourage employees to think about what they want their retirement to look like, how much annual income is required to support that vision, and consider what the firm can do to support them in terms of financial contributions.

Pension contribution limits:
Employees trust you to help them make the right financial decisions so it is important that the firm provides clear guidance on the potential pitfalls of pension contribution limits. Providing clearer communications can help instill trust whilst also removing potential financial stressors.

Flexi-access drawdown 2017/18.
Over 55-year-olds are entitled to draw a pension whilst still working via flexi-access drawdown. However, they can only put up to £4,000pa into their pension if they are doing this, reduced from a £10,000pa limit in 2016/17.

The Tapered Annual Allowance 2017/18.
The standard annual pension contribution limit stands at £40,000. This will be reduced by £1 for every £2 of 'adjusted income' over £150,000 in a tax year, to a floor of £10,000. Individuals must also retrospectively calculate their pension contributions for 2016/17 to ensure completing accurate tax returns.

Where to begin?

Properly structured risk and benefit audits can prove essential, ensuring relevance and compliance, not to mention cost savings. In Gallagher's experience, many risk audits can end up saving a company significant sums in terms of identifying and mitigating potential tax and uninsured liabilities.

Meanwhile, ensuring the firm's benefits strategy is keeping pace with the shifting environment requires a combination of workforce insights, plus strategic consultancy to identify barriers to engagement with employees and ways to tackle these barriers.

At a time when recruitment and retention is becoming ever more challenging, it pays to get - and stay - on trend. Get in touch with a Gallagher specialist to see how we can assist.

TO FIND OUT MORE ›

STEWART IRELAND
Sales & Marketing Director, Employee Benefits
+44 14 8335 8327 | Stewart_Ireland@ajg.com

06. THE STRATEGIC USE OF LEGAL INDEMNITY INSURANCE

Legal indemnity insurance has been a way to mitigate title risk for many years, however the insurance market is changing. Even in a scenario where there has already been a complainant, insurance can still be considered with an excess on the policy.

There are instances where even if litigation costs are recoverable, the financial impact of project delays and potential loss of earnings might not always be guaranteed. Our Legal Indemnity team highlight two scenarios based on recent, well-known cases to show how the insurance could have played a strategic role.

The scenario: Carillion and the awarding of public contracts

The collapse of Carillion has brought the Public Services Act back into the spotlight, raising risks to developers and contractors working with local authorities. Much more than a construction company, Carillion badged itself as an 'integrated support services business.' In 2016, Carillion had sales of GBP5.2bn, with an impressive market capitalisation of almost GBP1bn. The following year, the company collapsed under the weight of GBP1.5bn of debt. Its demise led to questions as to how the company had continued to secure new contracts from local authorities, and has led to a review of the process for the awarding of large contracts.

The Public Services (Social Value) Act forces the Government to consider the social consequences of awarding contracts to large companies. At least 25 local councils had contracts with Carillion, including catering, cleaning, major engineering, library management and road gritting. The issue was that Carillion could not provide so many specialist services, which over time became a systemic risk.

Using the Public Services Act, a bidding company which was unsuccessful in the awarding of a bid has the right to challenge the decision of the local authority. This can cause many problems for the winner of the bid, such as project delay and additional costs, especially if an awarded bid is cancelled and a second tender issued.

Many of the risks that emanate from a property transaction, refinancing, or development can be insured. Legal indemnity insurance protects against the risk of third party claims arising from a legal defect or challenge to the development or ownership of assets. In this challenged bid scenario, the policy could cover:

- Legal fees and court costs that the winning bidder incurs as a result of defending a challenge from another bidder;
- Project expenses (that the winning bidder was contracted to spend) incurred before the challenge was made;
- The profit that the winning bidder was likely to make should they lose the project as a result of the challenge;
- Bid costs for the second tender held as a result of the challenge.

The scenario: Chelsea Football Club and Rights of Light

In early 2018, the courts ruled that a project backed by Chelsea Football Club for a new stadium could continue; following a four year delay caused by one local family's opposition to the project on account of a rights to light claim.

In 2014, the club had developed plans to create the world's most expensive stadium. The plans were granted planning consent by the local council, and had received the backing of the London Mayor, as the project was anticipated to bring an economic boost to the local area. However, on account of the size of the proposed stadium, the project would have infringed the right to light for many neighbouring properties.

Although the club agreed to compensate 50 of the neighbouring homes, they reached an impasse when a local family, opposed the project and secured a High Court injunction. Despite two years of negotiation, the club's lawyers wrote to the council saying the family's opposition posed a clear risk, and funding had been on hold. Using Section 203 of the Housing and Planning Act 2016, local councillors then overrode the injunction as the project was deemed to be in the wider 'public interest.' Councillors voted to buy the disputed land, and then lease it back to the club so that the project could proceed.

Despite Section 203 providing for compensation to claimants, the family did not back down. A legal battle ensued and was resolved only in January 2018, after four years of delay.

In circumstances like these a legal indemnity insurance policy could have been deployed. There are a number of ways that a policy can be structured. An "agreed conduct" policy allows for the developer to negotiate with named neighbouring properties and either an excess against the policy or an excess against each property in place. Any expenditure over and above the excess will be borne by the insurer. Alternatively, the policy can be designed with a "wait and see" structure, whereby the developer does not flag rights of light and the policy will respond in the event that a claimant comes forward. Generally, there is no excess on these policies.

In the case of Chelsea Football Club, the family would have received a compensation sum. The policy would cover this (over and above any agreed excess) and the associated legal fees of the case. The insurance also would have covered the delay to the scheme, and any future loss of profit to the club as a result of this delay, including increased interest payments, increased plant costs, any contractual penalties, increased security costs and wages and salaries of staff.

Legal Indemnity insurance can assist with ensuring that a transaction, development, or refinancing closes by providing comfort that there is recourse against an insurance company in the event that a claimant comes forward. This enables lenders, purchasers and tenants to mitigate the risks associated with the development, ownership, and use of an asset, with a timely and cost effective solution.

Gallagher's Legal Indemnity team is experienced with working to tight timescales, delivering complex transactions and developments. Our clients include law firms, property owners and developers. Our experience enables us to provide advice and comment on the availability of products, coverage and premium rates to assist you quickly and thoroughly without any unnecessary delay. In some cases, we can put coverage in place in as little as 24 hours, making this a solution that can be rapidly deployed to support your clients.

TO FIND OUT MORE ›

ANNA BEADSMOORE
Head of Legal Indemnity
+44 (0)20 7234 4618 | Anna_Beadsmoore@ajg.com

07. THE CHANGING MARKET FOR WARRANTY & INDEMNITY (W&I) INSURANCE

W&I insurance has historically been prevalent within certain sectors as transactors recognised the strategic benefits to be gained from limiting their liability.

On the sale side, the cover effectively allows the seller to limit their liability to £1 and make a completely clean exit from a transaction. Conversely, the buyer policy allows the purchaser to claim directly from the insurer in the event of a breach of warranty by the seller, regardless of any rights they have in the Sale & Purchase Agreement (SPA) to pursue the seller.

However, W&I cover has traditionally been met with resistance by some circles of the legal community. It must be said that, until recently, the process of arranging W&I insurance was cumbersome, costly, and onerous. It became evident for more complex transactions that insurers needed every stone unturned in order to provide coverage for certain warranties. Markets would also predominantly be attracted to certain sectors on account of preferable risk profiles, while other sectors fell outside the appetite of insurers - leaving transactors unable to secure cover. It is therefore understandable that in some cases, lawyers were unwilling to highlight the coverage available to their clients.

That said, in recent years - and particularly in the last six months - the W&I and Tax Insurance market has evolved dramatically. Market capacity has tripled in two years with 23 insurers offering W&I cover in almost all jurisdictions and sectors globally. Insurers can no longer 'pick and choose' the deals that they want to underwrite and have had to become far more commercially minded in respect of premium, breadth of coverage and efficiency of process. In short, the W&I insurance market has listened the concerns of transactors and their lawyers, and have worked to make the product far more relevant and palatable.

Take price as the first example of change; W&I rates have dropped from circa 1%-2% several years ago, to 0.5%-1%. Minimum premiums required by insurers have dropped from £100,000 to £25,000 in the last three months alone. Average excess levels have also reduced dramatically, from 1.5% in 2015, to between 0%-0.5% today (depending on the sector). Insurers are becoming wise to the fact that, due to the sheer volume of new entrants to the market, there is significant competition for every M&A deal that comes to the market and as such, they need to be aggressive in setting their rates in order to secure new business.

In terms of coverage, 'low risk known issues' (that were previously excluded as standard) are now being included within coverage as the race for differentiation amongst insurers continues. These known tax risks that had the potential to derail deals in the past, are now being included at no extra cost - predominantly due to the fact that there are more tax underwriters in the market and the experience of underwriting these risks has broadened over the years.

Finally, the process itself in respect of placing insurance for a transaction has become far less cumbersome. On account of competition, insurers realise that their reputation is at stake if they take too long to consider and finalise cover. As such, the vast majority are willing to take more of a strategic view on certain items that may previously have delayed coverage being put into place; in the past, insurers wanted sufficient time for extensive due diligence to take place. Today, insurers will still expect to see due diligence completed for areas being warranted, but they are becoming more accepting of internal financial and tax due diligence - provided these are in a report form and carried out by individuals with the necessary qualifications to do so. On overall timing and speed of placement, insurers are now able to get fully tailored, fully negotiated policies in place within 5-7 working days of first contact with the transactors, or law firm.

As a result of these changes, W&I insurance should now be a consideration for any single private transaction, regardless of jurisdiction or industry. There are immense benefits to be gained by both buyer and seller alike, and now that the coverage is broader, better priced, and far quicker to transact, we recommend that lawyers speak to us when they have a M&A deal on the table, to see how Gallagher might be able to assist.

TO FIND OUT MORE ›

CHARLES RUSSELL
Head of Transactional Risks
+44 (0)20 7204 6237 | Charles_Russell@ajg.com

CONDITIONS AND LIMITATIONS

This information is not intended to constitute any form of opinion or specific guidance and recipients should not infer any opinion or specific guidance from its content. Recipients should not rely exclusively on the information contained in the bulletin and should make decisions based on a full consideration of all available information. We make no warranties, express or implied, as to the accuracy, reliability or correctness of the information provided. We and our officers, employees or agents shall not be responsible for any loss whatsoever arising from the recipient's reliance upon any information we provide and exclude liability for the statistical content to fullest extent permitted by law.

Gallagher

Insurance | Risk Management | Consulting