CYBER RISKS

FOR CONSTRUCTION AND FACILITIES MANAGEMENT CONTRACTORS

CONTENTS

INTRODUCTION

Reports of a new cyber risk or attack are never far from the headlines. This evolving threat is omnipresent for UK businesses. It ranked highest in the UK in Allianz's 2018 Risk Barometer[1] and was reported as a key risk by over 60% of participants. In the same survey, 54% of respondents identified cyber as the most underestimated risk.

These are not empty fears. In 2016, the Home Office's Commercial Victimisation Survey[2] (circa 1,000 respondents) showed that online crimes affected 15% of construction businesses. It was reported that 71% of cases arose from computer viruses and 10% from malicious hacking.

AN INCREASING THREAT

Since the 2016 survey, we have seen a significant increase in ransomware attacks. The estimated global cost in 2016 was USD 1 billion; this increased to USD 4 billion in 2017. The WannaCry and NotPetya attacks in May and June 2017 show that malware has the potential to cause and spread issues across the globe.

The regulatory landscape is changing too. With effect from 25 May 2018, the EU General Data Protection Regulations (GDPR) apply to UK businesses. This impacts all data controllers and processors that reside within the EU, with identical provisions applying in the UK. Importantly, its territorial scope is wider than the EU. GDPR applies to the processing of personal data of data subjects who reside within the EU by both controllers and processors where they offer goods or services to people in the EU or monitor their behaviour.

While it may feel that this is a problem that predominantly affects the US, this is more likely a result of the stricter reporting and notification requirements in that jurisdiction (see page 8).

It is also worth mentioning that data need not be exclusively electronic and the regulations are equally applicable to traditional hard copy records. This important regulatory change is dealt with in more detail within this paper.

CONSIDERING THE ISSUES

Within this report, we highlight some of the risks faced by the construction industry and the opportunities for transferring risk to the insurance market. We recognise that this risk has many different aspects for businesses. For example, facilities management (FM) contractors have considerable exposures in relation to their interface with networked building management systems (BMS), the Internet of Things (IoT) and, in the case of certain soft FM activities, the handling of personal data.

We conclude our paper with an overview of the coverage available under a cyber policy in comparison to more traditional insurance coverage. As with any insurance product purchase, relying on an off-the-shelf insurance product without fully considering your unique risk characteristics is a dangerous strategy; standard policies may not include the coverage required for your business.

1 *Allianz 2018 Risk Barometer*

2 *Home Office 2016 Commercial Victimisation Survey*

CYBER RISKS FOR CONTRACTORS

All modern businesses are increasingly reliant on both technology and data. Construction and FM contractors face unique risks from cyber threats, be these malicious attack or system errors, given the value of the information they hold on their projects and critical infrastructure. These businesses can struggle to identify and evaluate strategic cyber risk – risks that pose existential threats to their businesses. Cyber threats must be defined with potential exposures measured in terms of operating income, revenue or profit to truly understand the magnitude of the risk.

While advances in technology are transforming every aspect of the construction industry, there are four key areas which need to be considered by most businesses:

1. The most obvious example is building information modelling (BIM). By developing a 3D model of a project in real time, BIM improves efficiency throughout the entire project lifecycle. According to a recent study[3], BIM users can reduce 5% of their total construction cost and attain 25% improvement in labour productivity. Many governments are strongly encouraging, or even mandating, the use of BIM for complex projects to allow contractors to exchange information electronically.
2. Ransomware and malware attacks, while not affecting IoT or BIM data, have the ability to disable Windows-based hardware to the extent that they are unusable or must be completely reset.
3. Advances in technology, along with the evolution of the IoT, also impact a contractor's cyber risk profile. These projects incorporate elements that are increasingly complex and connected to the outside world. In addition, the equipment being used to construct these projects is being revolutionised, from robotic bricklaying to autonomous vehicles.
4. New technology is also revolutionising the management of health and safety on construction sites[4]. The capture of this data, particularly in relation to the health of the workforce, brings additional risks in relation to the control and processing of sensitive personal information.

Companies are encouraging a more mobile workforce, with the use of laptops, tablets and smartphones on the increase. Networks that conventionally had defined borders are expanding. These increased complexities mean companies need to be aware of not only what is happening within their network, but also have visibility of external connection points, mobile and laptop access, subsidiary organisations and other interconnections.

3 *Dodge Data & Analytics' study: The Business Value of BIM for Infrastructure 2017*

4 *JLT Specialty Thought Leadership: How Technology is Improving Safety in Construction*

These risks can impact an organisation's balance sheet in a number of ways. First party losses can arise from the cost of reinstating data or demands for money through ransom attacks. These losses can be substantial and may also extend to re-creation of lost data, extra expense and overtime. Imagine the additional cost to a project following a ransomware attack on an architect or other professional consultant that requires designs to be recreated from scratch.

The losses from a competitor accessing your intellectual property may be harder to quantify.

Third party losses can arise through contractual or common law liabilities where damages are payable to, say, a customer whose data is compromised by insecure systems or data breaches.

Finally, there is the regulatory liability, increasingly relevant in the UK and EU with the implementation of GDPR, discussed later in this paper.

CASE STUDY 1

CONTRACTOR PROVIDES A GATEWAY TO ASIO FOR CHINESE HACKERS

It has been widely reported that the design layout of a top secret intelligence facility was stolen from an Australian construction company by Chinese state-sponsored hackers.

The Australian Security Intelligence Organisation (ASIO), the country's domestic spy agency, suffered the security breach when an attack on a building contractor exposed the building structure, layout, electrical services, communication systems and computer networks.

Leaving aside the costs the contractor incurred, it had significant questions to answer about the breach and its security protocols. There was also substantial reputational damage as a result of this media-reported, high profile incident.

SPECIAL CONSIDERATIONS FOR CONSTRUCTION BUSINESSES

Many of the headline-grabbing cyber breaches focus on the customer impacts in the business to consumer (B2C) environment. Think of an infamous cyber-attack and you will probably recall the 2014 TalkTalk breach in the UK or the Target breach in the US in 2013. However, the business to business (B2B) space also represents a significant risk through lost business opportunities.

A study facilitated by Harvard Business Review Analytics Service, JLT and Business Insurance found that 58% of respondents rated cyber threats as a significant or very significant risk to their future business relationships. This statistic becomes more interesting when contrasted with 52% of businesses citing lawsuits or threat of legal action of significant concern[5]. These results align with Cisco Systems' 2017[6] findings which revealed one in four businesses that experienced a breach lost business opportunities as a result.

In the B2B context, cyber risks pose significant concerns to construction and FM businesses. Consider the following:

1. CONTRACTORS ARE NOT ALWAYS THE TARGET

In the previous case study (page 5), the contractor who suffered the breach which led to the disclosure of highly sensitive client information was not the end target. 'Gateway' businesses present a rich target for both nation state and criminal cyber actors seeking information or to cause disruption. As we have seen with WannaCry and NotPetya, malware attacks in particular are progressing in sophistication and are increasingly used for disruption or destruction rather than financial gain or accessing personal data.

Contractors have to consider the risk of network interruption or ransomware attacks in terms of business delivery. In addition, they face particular risks from such attacks during bidding processes when there is no flexibility in relation to deadlines. An attack during the tender process, even if it is only a partial attack, not only puts the potential revenue of the project at risk but also the (often significant) costs to develop the bid itself.

2. CONTRACTORS' DESIGN DATA IS INTELLIGENCE

Confidentiality and safeguarding sensitive information or intellectual property is critical for construction businesses. They possess information that is of tremendous value to a wide variety of nefarious actors. Design and engineering specifications represent valuable 'intelligence' which provides a strategic advantage to these actors. Again, the ultimate target of the action may not be the contractor itself, but the contractors' client.

5 *Managing Cyber Risk: Understanding the Opportunity*

6 *The Cisco 2017 Annual Cybersecurity Report*

3. CONSTRUCTION FIRMS' INTANGIBLE RISK CAN TRANSLATE TO TANGIBLE IMPACT

The ability to target critical infrastructure, airports, key buildings or sensitive facilities means that the loss may be more than simply the potential exposure of information for these organisations.

Potential impacts extend to include interruption of critical functions, physical damage, subsequent social engineering and extortion opportunities. At the far end of the spectrum, there is the ability to combine a physical attack with a virtual one.

4. CONTRACTORS POSE BROADER RISK IMPACTS

The number of parties impacted in a cyber incident is not limited to just the contractor and its direct clients. Any of the parties involved in planning, designing, implementing and operating the affected project could be entangled in disruption caused by a cyber incident.

The Cisco 2017 Annual Cybersecurity Report[6] notes that operational capabilities are most likely to be affected by a public breach. Delays, extra expense and workarounds may be necessary if project details are exposed, unavailable or destroyed. Shared systems like BIM platforms present challenges where security is the shared responsibility of all parties with access.

Though advantageous for collaboration, an intrusion for one participating organisation could easily impact the other parties. Cisco's report[6] further notes, "Organisations must look at their value chain holistically and consider whether each third-party that is involved in their business model or touching their offerings poses a risk to their security." It is important that subcontractors and suppliers conform to your own data security standards.

CASE STUDY 2

ENSURE YOUR PROCESSES CONSIDER GATEWAY RISKS

Some subcontractors impose less vigorous standards when investing in and implementing risk management protocols. This is equally true in respect to technological threats. Hackers may look to enter a larger or more complex business system down the supply chain where the protection is less extensive.

In 2013, hackers famously accessed the network of US retailer Target Corporation through the network credentials of Fazio Mechanical Services, a contractor that provided refrigeration and HVAC systems to Target Corporation.

The hackers installed malware in the security and payment system and were able to steal 40 million credit and debit card numbers, in addition to 70 million customer records. The data breach cost the retailer circa USD 300 million in addition to the immense reputational damage the company suffered.

5. PREPARE FOR TRADE-OFFS BETWEEN CONNECTIVITY AND SECURITY

The very nature of the construction and FM sectors involves the sharing and transmission of critical and sensitive data.

In exchange for the communication benefits, firms are exposed to more cyber-driven risks than ever before as a result of:

- Increased connectivity
- Reliance on digital assets
- Technological vulnerabilities
- Interdependence with joint ventures
- Increased value of intelligence as a currency
- The pervasiveness of malicious actors.

The impacts of cyber risk can potentially include monetary costs to the firm, reputational harm, third-party financial loss, physical damage and bodily injury, among others.

6. A CONTRACTOR'S CREDIBILITY IS AT RISK

The importance of confidentiality creates a massive potential for reputational damage should a breach occur.

An organisation's reputation is built on trust from clients, partners, subcontractors and others. A cyber event disrupting project progress or exposing confidential information would severely tarnish the firm's reputation and could thwart future opportunities. Cisco's 2017 report[6] notes 42% of IT security personnel saw a substantial loss of opportunity while 39% saw a substantial loss of customers due to adverse media publicity following an attack.

7. THE COSTS CAN BE FAR REACHING

The contractor or FM company may incur substantial first party costs to rectify or mitigate issues arising from a cyber event, as we have already detailed on page 3. In addition to these first party losses, claims can also arise from others.

Third parties, including clients, subcontractors and suppliers, can also be affected. They may incur costs or suffer damages due to a cyber event and the contractor or FM company could be responsible for these as well.

There is also the potential to incur fines arising from a breach of applicable regulations.

UNDERSTANDING REGULATORY REQUIREMENTS

The most developed market in relation to regulating cyber risks remains the US. Based on headlines, it may even seem as though the majority of data breaches that take place occur in the US. This is not actually the case and is just a product of the notification environment: 47 of the 50 states have mandatory data breach notification requirements. Consequently, cyber events in the US are more widely publicised and scrutinised. As cyber risk becomes a greater concern globally, more territories are implementing new, or more onerous, data protection regulations.

The EU's GDPR was implemented in May 2018. This applies to all controllers and processors of EU data; it includes the UK both before and after Brexit. The implications are summarised below.

KEY CHANGES	IMPACT
INCREASED PENALTIES	
In the event of a data breach, organisations are subject to the regulation's penalties and notification requirements from 25 May 2018.	The Information Commissioner's Office had the power to issue fines up to GBP 500,000 under the Data Protection Act 1998. GDPR increases the maximum fine to 4% of global turnover or EUR 20 million; whichever is the larger. This represents a substantial business risk and requires data security to be addressed at board level.
COMPULSORY REGULATORY NOTIFICATION	
GDPR requires compulsory regulatory notification of personal data breaches likely to result in harm to data subjects within 72 hours. When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller is required to notify the affected individuals "without undue delay". **Although the obligation to notify is conditional on awareness, data controllers are required to implement appropriate technical and organisational measures as well as a process for regularly testing, assessing and evaluating the effectiveness of those measures to ensure the security of processing.**	This is a significant break from the past where there was no requirement in the EU to inform the public of a data breach for the majority of organisations. This requirement brings the EU and UK legislation closer to the US provisions and is expected to increase public awareness of breaches. A well-documented incident response plan will be essential to ensure compliance.
NEW DATA PROCESSOR RESPONSIBILITIES	

KEY CHANGES	IMPACT
Under GDPR, data processors have direct responsibility when handling personal data. **Previously, data controllers were only accountable when working with personal data.**	Organisations are advised to conduct a detailed review of existing contracts with suppliers who provide data processing services ahead of GDPR adoption. Organisations should make sure data processors only process information following instruction from a data controller and they obtain assurance that these instructions are being met.
EXTENDED RIGHTS FOR DATA SUBJECTS	
One of the main ambitions of the European Commission in proposing a new data protection framework was to bolster the rights of individuals. This is clearly reflected in the strengthened rights of data subjects. **Strengthened rights include the right to be forgotten, the right of access to personal data and its correction where it is inaccurate. There is also a right to restrict certain processing and a right to object to personal data being processed for direct marketing purposes.** **Individuals can also ask to have their personal data sent back in a structured and commonly used format so that it can easily be transferred to another data controller (this is known as data portability).**	The data controller is obliged to permanently erase personal data under certain circumstances. This requires a review of both processes and technology solutions to ensure that both paper and electronic records can and are erased in accordance with retention requirements and requests. This also applies to records which are stored in historic archives.

More information in relation to the changes and the impact on businesses is available at https://www.jltspecialty.com/cyber-decoder-GDPR

RISK ASSESSMENT, EVALUATION AND MANAGEMENT

It's often said that insurance is only one aspect of risk management and should not be used until the risk is evaluated and other risk mitigation measures have been deployed. Relying on an off-the-shelf insurance product without fully considering a company's unique risk characteristics is a dangerous strategy as many of the standard policies may not include the coverage(s) required for the business.

Cyber risk varies by incident and by organisation. Identifying and understanding the risks, whether insurable or not, is an imperative part of the process. As FireEye's 2018 M-Trends report[7] notes, "[organisations] need to examine every possible scenario and have playbooks ready to implement." We have also already identified in this report how organisations should evaluate risks in terms of their impact on the business; both the first and third party implications to revenue, operating income and profit.

DEVELOP PROCESSES AND PROTOCOLS TO ENSURE COMPLIANCE

Considering cyber exposure will increasingly become an integral part of planning, management and operation of a construction company's robust policies and processes. The most important first step to protection is to understand the sensitive information and technology a business uses and relies on.

Secondly, internal due diligence around controls, processes and procedures must be in place to mitigate or minimise vulnerability. One very important, yet often overlooked, area of risk is the human element. Employee education around good cyber hygiene is just as important as the firewalls that are put in place. Training can also help to reduce a company's vulnerability to phishing attacks, which have been on the rise. Practising a culture of awareness is crucial to avoiding attacks and minimising their impact.

In addition to evaluating risk within an organisation, it is crucial to understand who the business may be connected to at each level of a project and in support of general business activities. Any outside organisation with access to a company's data or technology represents a potential exposure. Contractors and FM companies must understand and evaluate cyber security within their supply chains before considering and planning for external weak links.

HAVE A PLAN TO RESPOND TO A CYBER EVENT

In order to minimise the impact of a cyber incident, contractors and FM companies should develop (and test) an incident response plan.

The plan should provide for a prompt response when a prospective cyber incident has been flagged and the initiation of a crisis management protocol to help minimise the potential for damage and loss.

7 *FireEye M-Trends 2018 Report*

TRANSFERRING CYBER RISK TO INSURERS

Once cyber risk has been evaluated and mitigated where possible, there is the option to minimise the impact of a potential event through insurance. Coverage is available under professional indemnity (PI), third party liability (TPL) or cyber insurance policies.

TAILORED CYBER INSURANCE POLICIES

Cyber insurance provides both first party and third party coverage following a cyber event such as a security failure or privacy incident. The coverage is purchased on an 'a la carte' basis and is therefore tailored to an organisation's particular risk management strategy and goals.

The core first party coverage elements include:

- Breach response costs (such as IT forensics, public relations assistance, notification costs and legal advice)
- Cyber extortion costs such as ransom payments
- Information asset restoration (to restore, recover or replace damaged or destroyed information assets)
- Network business interruption costs such as lost business income and extra expense. This cover can be particularly valuable for insureds that are reliant on data or technology.

In the event of a network intrusion that renders project plans or details unavailable, there could be significant incident response costs, such as computer forensics. Specialist firms work in aftermath of a breach or hacking event to determine the scope of damage to the computer systems, the nature of the malware and assist in the restoration of corrupted data and systems. Forensics costs can escalate quickly; one JLT client spent in excess of GBP 1 million in a week and GBP 1.75 million within five weeks on this service alone.

Following a cyber event, an organisation may face liability for failure to safeguard information or causing financial loss to a third party. A cyber policy would include third party coverage elements applicable to damages and defence costs in the event of a claim, as well as cover for defence of privacy regulatory proceedings and penalties (where these are insurable by law).

When used in conjunction with the risk transfer component, cyber insurance policies can also align insureds with expert breach response vendors to deploy the services outlined above, such as IT forensics, notification, public relations and legal advice.

Another developing risk transfer solution for construction and FM contractors is reputation indemnity insurance. This policy can provide protection against lost revenue or profit arising from negative publicity following a cyber attack or loss. Given the rate of development for this bespoke coverage, we have not included it within the analysis of policy protection available.

Finally, it is important to note that, in response to the growing cyber terrorism threat, Pool Re has agreed to provide a cyber extension to its Great Britain terrorism cover for material damage risks. This change took effect from 1 April 2018.

CONSTRUCTION COVERAGE GAP ANALYSIS

Below we have reviewed cover available under typical PI and TPL policies and summarised the coverage against cyber risk scenarios.

● = Coverage Likely ● = Coverage possible, but with issues ● = Coverage Unlikely

COVERAGE SCENARIO / ITEM	PI	TPL	CYBER POLICY
Misdirected digital communications	●	●	●
Breach of employee information	●	●	●
Breach or theft of mobile devices	●	●	●
Breach or theft of offline confidential information	●	●	●
Breaches caused by third party vendors	●	●	●
Breaches of third party confidential corporate information	●	●	●
Business interruption due to system failures (no physical cause)	●	●	●
Business interruption triggered only by cyber attack	●	●	●
Media liability	●	●	●
Contractual indemnification obligations for customer data breach expenses but not liquidated or ascertained damages (LADs)	●	●	●
Contractual obligations to maintain security following an incident	●	●	●
Crisis expenses such as forensic consultants, credit monitoring, consumer notification, crisis consultant, public relations consultant, call centre (statutory)	●	●	●
Data restoration and re-creation after failure or violation of IT systems	●	●	●
Cyber-attacks perpetrated by terrorist organisations	●	●	●
Hacks by malicious outsiders	●	●	●
Third party intellectual property infringement (including patent)	●	●	●
First party intellectual property infringement	●	●	●
Phishing scams resulting in leaked information	●	●	●
Regulatory investigations due to privacy law violations	●	●	●
Social media account compromise	●	●	●
Social media content liability	●	●	●
Theft of information by rogue employees	●	●	●
Theft of money or securities due to cyber attack	●	●	●
Wrongful disclosure of information orally	●	●	●
Physical damage caused by a cyber attack	●	●	●
Bodily injury caused by a cyber attack	●	●	●

The general conclusion from this analysis was that while insureds may be able to rely on existing insurances to respond to cyber losses, there are numerous uncertainties that will persist. A specific cyber insurance product delivers a more certain and robust solution.

NOTE: This analysis has been carried out on typical wordings. Please get in touch with your usual JLT Construction contact if you would like more information, access to a more detailed coverage analysis or for a detailed review of your policy wording.

CONTRACTUAL REQUIREMENTS FOR CYBER INSURANCE

We have not yet experienced any widespread requirements within building of FM contracts obliging the contractor or service provider to maintain cyber risk insurance. We would be interested to know if any clients or prospects have encountered these conditions, to what limit the principal requested protection and on what specific terms.

To discuss this aspect further, please contact **Mike Johnson** (mike_johnson@jltgroup.com) or your usual contact at JLT Construction.

SUMMARY

BE AWARE AND PROACTIVELY REDUCE YOUR RISK

While taking advantage of the efficiencies achieved through technology implementation, contractors and FM companies must be aware of the ways in which technology creates increased risk exposure. A sound approach to risk management can prove to be a differentiating factor over the long run for a company.

On this basis, insurance should be seen as only one individual tool at the risk manager's disposal. The specific circumstances of each loss will determine the extent to which policies will respond. Our analysis has determined that while there may be partial protection under existing products, these risks are best addressed through a properly designed, specific cyber product.

OUR CAPABILITIES

Each industry sector faces a unique blend of cyber risks. Ignoring them, or even playing them down, could be catastrophic, both financially and in terms of a company's reputation.

For 30 years, JLT Construction has worked in partnership with clients, delivering unrivalled service and innovative solutions that shape all areas of construction insurance. With more than 135 experts, the team works across the breadth of building, civil works, engineering risks and facilities management.

Now, the Construction team's industry experts have joined forces with our Cyber team to present clients and prospects with the best of both worlds. They enjoy market-leading expertise in the industry and cyber risk issues that confront contractors.

JLT works with companies every day to help them better understand their potential exposures. We help them identify, assess and quantify those exposures, and then design innovative insurance programmes to help mitigate those risks.

Using our expertise and imagination, we challenge the accepted industry norms to deliver pre-eminent products, at the best price, underwritten by the right insurers.

At JLT Specialty, we believe in doing things differently.

Why? Because in the world of insurance broking, risk management, claims consulting and settlements, the only way we can develop solutions, which really deliver, is to fully understand all of the different challenges our clients face. And we know the answer does exist, no matter how difficult the question is.

Our success comes from focusing on sectors where we know we can make the greatest difference. On using insight, intelligence, and imagination to provide expert advice and robust – often unique – solutions. And on building partner teams to work side-by-side with clients, our network and the market to deliver responses, which are carefully considered from all angles.

Because of this approach, our clients trust us. They have total confidence in knowing the vital elements of their operations are covered, enabling their businesses to be even more ambitious and surpass expectations.

We know how we work makes us different. It's quite a claim but we're driven to deliver on it every single day.

APPENDIX: GLOSSARY/REFERENCES

BUILDING INFORMATION MODELLING (BIM)

A process for creating and managing information on a construction project across the project life cycle.

BUSINESS TO CONSUMER (B2C)

Business or transactions conducted directly between a company and consumers who are the end-users of its products or services.

BUSINESS TO BUSINESS (B2B)

A process where one business makes a commercial transaction with another.

DATA CONTROLLER

A staff member who (either alone or jointly with others) determines the purposes for which and the manner in which any personal data is processed.

DATA PORTABILITY

A right that allows individuals to obtain and reuse their personal data for their own purposes across different services.

DATA PROCESSORS

A worker who processes data on behalf of a data controller.

DATA SUBJECTS

An individual who is the subject of personal data; in other words, the individual whom personal data is about.

FACILITIES MANAGEMENT (FM) CONTRACTOR

A professional management company focused on the delivery of support services for the organisations it serves.

FIRST PARTY LOSS (FPL)

A loss that involves an insurer and an insured (the first party).

INTERNET OF THINGS (IoT)

The interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data.

LIQUIDATED AND ASCERTAINED DAMAGES (LADS)

Fixed damages stated in a building contract that a contractor must pay an employer if completion is delayed.

MEDIA LIABILITY

Negligence in a company's media content and advertising, including websites, blogs and social media.

NETWORKED BUILDING MANAGEMENT SYSTEMS (BMS)

Control systems that can be used to monitor and manage the mechanical, electrical and electromechanical services in a facility.

POOL RE

The most significant provider of terrorism cover in the UK, backed by the Treasury.

THIRD PARTY LOSS (TPL)

A loss that involves another person or company (i.e., the third party) other than the insurer and the insured.

CONTACTS

MIKE JOHNSON

Contractor Group Leader, JLT Construction

+44 (0)20 7528 4759

mike_johnson@jltgroup.com

JLT Specialty Limited

The St Botolph Building
138 Houndsditch
London EC3A 7AW
Tel +44 (0)20 7528 4000
Fax +44 (0)20 7528 4500

www.jltspecialty.com