



Covernotes



Don't Neglect Your Duty of Care to Employees Working Overseas

Before Covid-19 Business Travel overseas was a staple diet of a companies client engagement and continuing to grow. It is too soon to predict when the pre-Covid levels may be reached again, but there will be an uplift as UK PLC re-opens and the desire for face-to-face contact is re-ignited.

For UK employers, organising for an employee to travel overseas on business is a process which should involve extremely careful planning. Under the terms of UK employment law, an employer, who requires an employee to travel overseas on company business, should be diligently analysing the precise responsibilities of that employee whilst abroad and assessing and mitigating any risks to their health and safety.

As Covid-19 continues to dominate global health situations, employers should also be seeking to reduce the worry that employees might experience, if needing to travel for work.

A thorough risk assessment is vital, with past case law highlighting that judgements will be made against

employers who fail to assess risks adequately and so endanger the life, health and wellbeing of their employees overseas. Companies have been found liable in various types of case in which employees have been injured or killed abroad. Examples of employer negligence have included failing to advise employees about the risks of malaria¹ and requiring employees to take unsafe modes of transport when visiting overseas sites in remote locations. The impacts, for a company which neglects to plan every element of their employee's protection, can be profound.

Best practice should consist of doing everything reasonably practicable to safeguard the employee. Attention needs to be paid to security awareness training and actors including the overseas country's climate, seasonal weather conditions, culture and customs, political stability, security issues, terrorism threat, crime level, social stability, Covid-19 situation, levels of hygiene – and even the type of electrical adapters or appliances required for compatibility.

Staying in touch with an employee abroad and ensuring they feel supported and part of the team is also vital and establishing which hours in which to do this, given time-zone differences, is also important. Not adding extra strain to the employee's situation should be the goal, and ensuring that their mental health is supported, the objective at all times.

Considering all the elements of an employee's safety and trying to support their medical care and wellbeing in the best possible way can be a challenge, which is why specific group personal accident and travel protection exists and can be provided to businesses seeking to extend their duty of care to workers abroad.

A group personal accident and travel plan is a holistic approach to employee wellbeing, suitable for businesses of all sizes and in any sector. Such cover typically utilises technology, such as online portals and Apps, to ensure the employee is assisted at all times, both before their trip and during it. It usually encompasses elements of awareness training, to prepare the employee for

¹<https://www.personneltoday.com/hr/safety-and-financial-issues-to-consider-when-travelling-for-business/>

For additional information
<https://www.aig.co.uk/globecover>
<https://www.chubb.com/uk-en/businesses/resources/future-of-business-travel.html>

specific factors they will find within a country and fill in any knowledge gaps. At a practical level, it gives them the means to rebook flights, if necessary, access translation and Embassy support and replace a lost passport or stolen cash.

Most importantly, this type of plan also provides the level of high-grade medical insurance cover that is required, including rescue and repatriation, if necessary. Plans offer compensation and care, should any injury occur and step in to support loved ones, if an employee tragically dies overseas. If they are hospitalised, the cover often provides for a service

to relay messages to friends and family, as well as providing counselling and support.

Furthermore, the policy should pay for other aspects associated with travel, such as cancellation of flights, trip curtailment and lost baggage.

With so much uncertainty across the globe at present, be that rooted in health, terrorism, crime or social and political situations, it is vital for businesses to keep a firm grip on their risk management and duty of care. There is no need to be caught out and suffer reputational damage, by letting your employees down, when having first-rate group personal accident and

travel insurance cover in place is so easy to do.

Having such protection for employees, as part of their support package, can also enable a business to attract and retain the best talent, in what may be a small skills pool.

.....

“ Specific group personal accident and travel protection exists and can be provided to businesses seeking to extend their duty of care to workers abroad. ”

Cyber Insurance: Why Buying Wisely is Crucial

Altering the way in which we view cyber insurance purchase and policies is the change we need to see, if more businesses are to save themselves from incurring irrecoverable losses and continuing to fall prey to cyber criminals.

All too often, cyber insurance is bought because it is a requirement for a contract or because a business fears the impacts of a data breach on third parties, such as its customers. Businesses, far too infrequently, put their own business first, to consider the potential harm that a cyber-attack could cause to them, or how they would cope. In addition, too few businesses have robust cyber-crime training programmes in place.

Due to press headlines and GDPR fines, much of the buying and selling of cyber insurance has been focused on the risks attached to data breaches, leading to the cover being viewed as typical insurance protection, rather than as a vital business service¹. Some lower-grade cover encourages this

approach, excluding service benefits that are so important for the many businesses that find themselves targeted by cyber criminals.

Businesses seeking better protection should consider the other elements to cyber insurance, which are often the most beneficial, particularly for SMEs (small and medium enterprises). One is access to expertise, often only offered by higher-quality cyber insurance policies. IT expertise is typically made available to victims 24/7, to assist with system lockouts and assets' decryption. Such experts can identify the type of attack, the software used, its origin and even who on the dark web may wish to bargain with you, to have your systems restored.

Most SMEs simply do not have this level of IT expertise on tap and flounder after an attack, or even multiple attacks, as SMEs are stepping-stones into the systems of 'bigger fish' and specifically preyed upon by cyber criminals. Criminals also know SMEs are often vulnerable, lacking both physical protection, such as firewalls,

antivirus software and VPNs, and the staff training to keep the risk at bay. If you fall prey to cyber criminals, you will be far from alone, with 65% of medium-sized businesses having experienced cyber-attacks in 2019-20.²

When an attack occurs, it often results in business interruption, immobilising operations, preventing customers from being served and crippling online sales functionality. Despite this, starter-level cyber insurance policies usually offer no business interruption compensation.

Customers and suppliers need to be quickly advised about recovery strategies and any implications for their businesses, by virtue of your attack. That comes at a cost, without cyber protection to cover such expenses. It can also mean reputational damage - hard to combat, without PR support, again often only provided as part of good quality cyber cover.

Not having robust cyber insurance protection, or only having cyber included within all-risks cover, can also catch out businesses that are victims of

¹<https://www.professionalsecurity.co.uk/news/interviews/cyber-stepping-stone/>

²<https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021>

crime. Through cyber-crime techniques such as phishing – an email which looks as though it comes from a legitimate and trusted source and which asks for sensitive information to be revealed – and whaling, where a person poses as a senior executive and requests the transfer of funds, huge losses can result. If theft is not an element of cyber protection, financial losses can be incurred.

Cyber criminals are expert at manipulating untrained and naïve staff, encouraging them to do exactly what they want, such as clicking on a malware link that will enable them to penetrate systems and steal information, not questioning an email's legitimacy or believing they've spoken to the MD, when artificial intelligence (AI) has only made it appear as though they have. With the development of AI, such fabricated conversations could constitute a growing threat.

Part of any risk management strategy has to include staff training and raising awareness of the cyber threat and cyber criminals' techniques. Ensuring employees know how cyber criminals operate, are always on their guard when it comes to cyber-crime and buy in to the cyber protection strategies that the business implements, is key. It is far easier to try to prevent a cyber-attack than to try to rectify systems after one.

The message is that simply having a cyber insurance policy will not prevent issues occurring, but positive action can reduce your risk.

If that fails, which it still might, having quality cyber insurance at hand can be the difference between accessing a little bit of help and having your own cyber recovery team at your disposal; between having some rectification, GDPR and investigation costs covered and knowing any business interruption and theft of company monies will not distress your company finances. Buy your cyber protection wisely.



Don't Run the Risk of Ignoring ESG Strategies

Environmental Social Governance (ESG) can no longer be ignored by any company since it was placed in the insurance spotlight by Lloyds' of London. Having already begun to dominate considerations within investment portfolios and the actions of publicly listed companies and influenced European insurer decisions, ESG is now very much centre stage.

ESG, a term first coined in the 2005 landmark study, 'Who Cares Wins', inspired by UN Secretary General, Kofi Annan, is rapidly shooting to the top of the agendas of investors, regulators, customers and employees, combining, as it does, the three central pillars of sustainability and societal impact – environment, social impacts and governance.

ESG investment decisions are increasingly focusing on a company's approach to climate change and the mitigation of their environmental impacts. There is also an emphasis on

clean energy, water, sanitation and land management.

Whilst 'social' has been the "poor relation" within ESG to date, commentators believe the global pandemic has changed this, with workforce issues moving up the agenda and injustices around working conditions now exposed. How companies manage diversity and inclusion, health and safety and other aspects of their human interactions can greatly affect public perceptions and share prices.

As with environmental and social impacts, 'governance' too has grown in importance. Malpractice is quick to be exposed in the media and social media, whether it relates to business ethics, tax affairs, fiduciary duty, competitive behaviour or other management failings.

Whilst ESG was already hugely important, combining elements of corporate social responsibility with Socially Responsible Investment, it is now being embedded within risk management and

.....
“ ESG investment decisions are increasingly focusing on a company's approach to climate change and the mitigation of their environmental impacts. ”

is already influencing the availability and pricing of insurance policies.

Lloyd's of London published its first Environmental Social and Governance Report in December 2020, subtitled, 'Our Plan for Becoming a Truly Sustainable Insurance Marketplace'¹. Within this report It announced its intention to set targets for responsible underwriting and investments, to help accelerate the transition from fossil fuel dependency to renewable energy. New insurance coverage for thermal coal mines and thermal coal-fired power plants, amongst other types of similar polluting enterprises, will not be available through its syndicates, from January 1, 2022. This wide-ranging report also highlights how a business's ESG risk

management will become increasingly influential with regard to its insurance terms and premiums.

With many elements of ESG potentially impacting on claims, from climate change-related flooding and natural disasters to health and safety failings, employee disputes and management accountability, Lloyds decision has a sound business rationale. Other members of the insurer community have taken similar action; France's biggest insurer, AXA SA, withdrawing insurance from a German utility giant, on the basis of its coal operations and slow progress with its carbon footprint reduction. In 2017, AXA became the first insurer to impose underwriting restrictions on coal-related businesses.

It stopped providing insurance for coal mines and plants in December 2020.²

With rapid change in the workplace and the ongoing pressures of climate change, the growing power of social media and the need for transparency, no business can ignore the need to get to grips with ESG strategies. Whether it be your investors, regulators, customers or employees, there is a need for you to ensure you have taken appropriate actions to show your ESG credentials. Doing so will help you to both flourish and maintain strong and affordable insurance coverage. If you need help with that process, please get in touch with us and we can help you in your Environmental and Social Governance journey.

¹https://www.lloyds.com/-/media/files/about/responsible-business/esg/lloyds_esgreport_2020.pdf
²<https://www.insurancejournal.com/news/international/2021/03/12/605014.htm>



Get the Right Insurance If Continuing to Work From Home

Working from home could be here to stay for roughly half of those UK workers able to do so.¹ A survey of 5000 UK working adults, by the University of Nottingham and Stanford University, has found almost one-fifth (19%) want to continue working from home for five or more days a week. A fifth wish to do so for two days a week; another fifth for three days a week.²

Many large organisations are now considering implementing a 3-2 plan, of three days working from the office and two from home. Hybrid working appears to be the future for many

businesses and Lloyds Banking Group will be trialling hybrid working for thousands of staff in late spring after their research showed 77% of employees would be positive about working from home two to three days a week.³

These trends will be witnessed throughout the economy and small and medium-sized businesses are also likely to have to offer working from home as an option, for at least some of the working week. The strength of the demand for working from home means it is likely to be here to stay for many, but with that come insurance implications.

During lockdowns, home insurance providers did not require homeworkers to amend their home insurance policies, but that situation may change once restrictions lift. Anyone leaving employment to start a home-based business definitely needs to review their insurance. Not telling an insurer about new and permanent working arrangements would be deemed not declaring a 'material fact', which could invalidate any claim.

Insurance needs to cover both equipment and the data and systems it holds and operates. Hybrid workers potentially take laptops and data on

¹<https://www.theguardian.com/commentisfree/2021/mar/21/research-working-from-home>
²<https://voxeu.org/article/working-home-revolutionising-uk-labour-market>
³<https://www.unleashgroup.io/2021/04/19/banks-on-board-hybrid-flexible-working/>

journeys to and from the office. They need to check carefully with their employer who is insuring this and who would be deemed liable should a data breach occur in transit. Leaving a laptop on a train, or logging into a hotspot without use of a VPN and then being hacked, could both have major repercussions.

If employees rely on their home insurance to cover office laptops and gadgets, they should check their policy covers portable equipment and that accidental damage cover is in place, to prevent losses after spillages or breakages. Accidental damage claims have increased significantly during lockdown and laptops frequently feature. Single-item limits also need to be sufficient.

Homeworking insurance pricing typically depends on whether work is just clerical, or involves clients and others visiting the property – something lockdown has prevented. A change in ‘use’ of the home could be significant. Any other ‘business use’ of parts of the home, such as kitchen or garage, could also affect a premium. Having business stock covered by home insurance is highly unlikely.

Small and medium-sized businesses should also focus on the cyber risks surrounding working from home, especially as 65% of medium-sized and

39% of all businesses suffered a cyber security breach in the 12 months prior to and detailed in the Gov.uk Cyber Security Breaches Survey 2021⁴.

Neither a Commercial Combined nor Home Property insurance policy may fully cover all computer risks, but the growth in homeworking has seen new insurance policies emerging. Some cover both installed and portable computer equipment at a core cover level and then enable the addition of other modules offering benefits, such as covering the costs of reinstating data with professional help, increases in the cost of working following a cyber-attack or incident, and issues caused by viruses, hacking and denial of services attacks. As your insurance broker we are able to talk you through the ramifications and remedies available in these situations.

Protect your homeworking equipment from all risks and not just from theft but also cyber theft, if you continue to work from home. Not everything is stolen in physical form and protecting against the virtual threat is increasingly important, particularly if business losses would result from not having the right protection.

Talk to us about the new flexible policies available and so you are minimising your exposures to a cyber-attack



.....
“ Leaving a laptop on a train, or logging into a hotspot without use of a VPN and then being hacked, could both have major repercussions.”

.....
⁴<https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021>

Why Engineering Surveyors Should Receive a Warm Welcome

As the UK eases out of its third lockdown, the importance of engineering inspections has probably never been as significant. Despite engineering surveyors having been ‘key workers’, COVID-19 has created a backlog of engineering inspections and problems in engineering surveyors gaining access to some sites.

With UK Plc now opening up businesses should look to rapidly reinstate statutory inspections through a planned approach, providing engineering surveyors with documentary evidence to show how machinery and equipment was maintained, whilst statutory inspections were not possible.

As life edges back towards normality, engineering inspections should be

at the heart of engineering and manufacturing companies’ risk management strategies, being paramount for worker safety and a compliance requirement under the terms of various regulations.

The PUWER (Provision and Use of Work Equipment Regulations) 1998¹ demand that health and safety risks arising from any type of workplace equipment are prevented and con-

.....
¹<https://www.legislation.gov.uk/uksi/1998/2306/contents/made>

trolled through proper maintenance.

The LOLER, (Lifting Operations and Lifting Equipment Regulations) 1998², specifically govern lifting equipment and anything used to lift or lower people and/or loads, such as overhead cranes, forklift trucks, platform hoists and passenger/goods carrying lifts.

Another highly focused piece of legislation, The Pressure Systems Safety Regulations (PSSR)³ 2000, requires a written scheme of inspection for systems where gas, steam or refrigerants are held under pressure.

Then there are the Local Exhaust Ventilation Plant (LEV)⁴ regulations, part of the Control of Substances Hazardous to Health (COSHH) 2002 regulations⁵, requiring employers to control airborne LEV contaminants and operate and maintain safe extraction systems.

An engineering surveyor is an individual who helps a company deliver its

legal compliance through inspections. In some cases, such as LOLER, the law will state the required interval between inspections but, in many other instances, the engineering inspector is the one who will determine the period of time covered by the 'safe interval', according to the type of equipment, its use, its environment and whether that encourages issues such as corrosion.

The engineering surveyor can not only enhance workers safety and reduce liability claims but also help save money. A strong commitment to engineering inspection demonstrates to an insurer that risks are well-controlled.

The engineering surveyor can similarly be a trouble-shooter, identifying potential equipment problems early and flagging these up, prior to major failure of plant or equipment and the resulting business interruption and downtime. Inspections can help

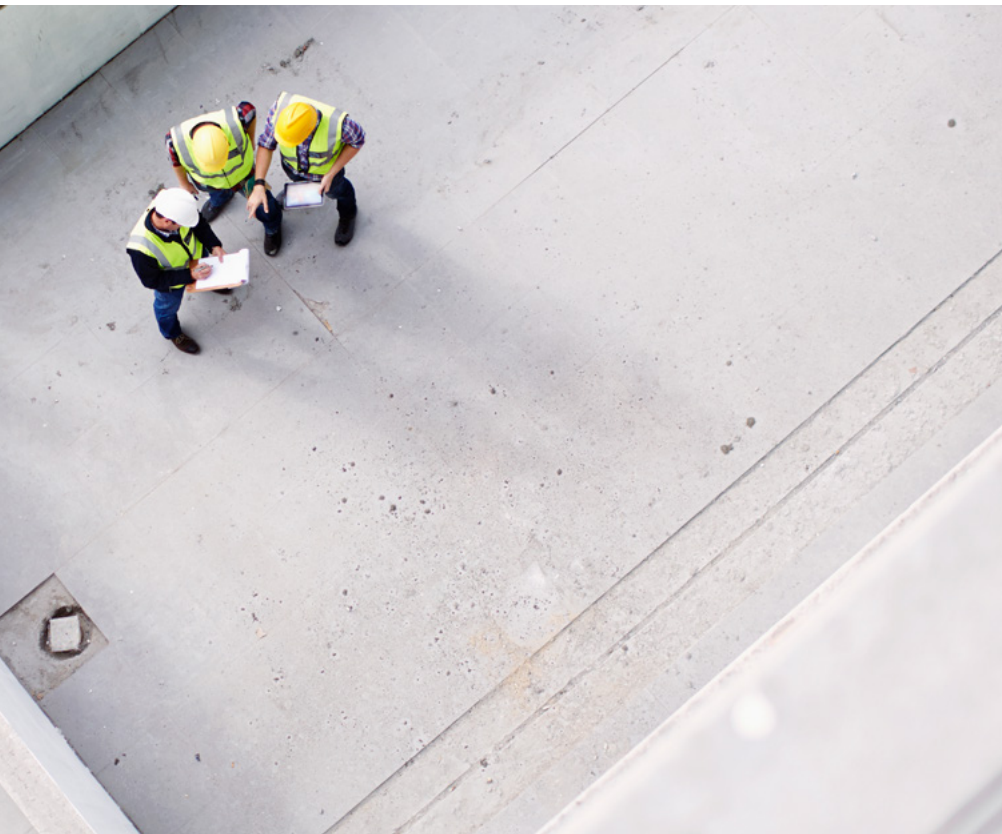
.....
“ A strong commitment to engineering inspection demonstrates to an insurer that risks are well-controlled. ”

a business plan their plant purchases more efficiently, as a result of their feedback regarding the life left in a piece of plant or machinery. Although inspections are not a replacement for maintenance, having regular insight from such surveys can keep a maintenance programme on its toes, identifying what needs to be done, potentially extending the lifetime of a piece of plant through an ongoing, enhanced maintenance approach. Engineering surveyors can also assist with the documentation required by some British Standards' certification schemes.

There are plant and equipment insurance policies which have a Sudden and Unforeseen Damage clause, to pay for breakdowns that could not have been predicted. Having engineering inspection records to support your claim that a breakdown was unexpected, can make a big difference.

Engineering surveyors can also carry out non-destructive testing, utilising dye penetrants, magnetic particles and ultrasonic testing, to identify issues with welds, casting, forgings, cracked surfaces and internal flaws in equipment or pipework, which are not externally visible.

However, in the post-Covid period, many engineering surveyors will prove their worth in testing equipment needing to be recommissioned following potentially extensive lay-offs. They



.....
²<https://www.legislation.gov.uk/ukxi/1998/2307/contents/made>
³<https://www.legislation.gov.uk/ukxi/2000/128/contents/made>
⁴<https://www.hse.gov.uk/lev/>
⁵<https://www.legislation.gov.uk/ukxi/2002/2677/regulation/7/made>

will also have a vital role to play in first in-service examination tests, also part of their remit, on new equipment possibly purchased with COVID-19 recovery grants and loans. The HSE has stated there is particular emphasis on this test for pressure systems, including boilers and combined heat and power systems, as this is “the checkpoint where the competent person determines if the written scheme of examination is adequate”, thus ensuring that safety integrity is not compromised.⁶

Duty holders in manufacturing and engineering companies who have had to delay their engineering inspections should welcome a return to a more normal inspection schedule for many reasons, not least because they will not solely have to rely on their judgement as to whether or not their equipment is safe. Having an inspector do that for you is truly valuable.



.....
⁶<https://www.hse.gov.uk/coronavirus/assets/docs/toler-pssr-during-outbreak.pdf>

.....
Hart Insurance Brokers
 10 James St
 Helensburgh
 G84 8AS

Tel: 0141 951 4100
 Fax: 0141 951 4101

www.hartinsure.co.uk
info@hartinsure.co.uk

Authorised and regulated by the Financial Conduct Authority

The information contained herein is not intended to constitute legal or other professional advice and should not be relied upon in lieu of consultation with your own legal and/or other professional advisors. Some of the information in this publication may be compiled by third party sources we consider to be reliable, however we do not guarantee and are not responsible for the accuracy of such information. We assume no duty in contract, tort, or otherwise in connection with this publication and expressly disclaim, to the fullest extent permitted by law, any liability in connection with this publication. Willis Towers Watson offers insurance-related services through its appropriately licensed entities in each jurisdiction in which it operates.

All rights reserved. Willis Towers Watson is a trading name of Willis Limited, Registered number: 181116 England and Wales. Registered address: 51 Lime Street, London, EC3M 7DQ. A Lloyd's Broker. Authorised and regulated by the Financial Conduct Authority for its general insurance mediation activities only.

Willis Towers Watson offers insurance-related services through its appropriately licensed and authorised companies in each country in which Willis Towers Watson operates, for example:

- In the United Kingdom, Willis Towers Watson Networks is a trading name of Willis Limited, registered number: 181116 England and Wales. Registered address: 51 Lime Street, London, EC3M 7DQ. A Lloyd's Broker. Authorised and regulated by the Financial Conduct Authority for its general insurance mediation activities only; and
- Willis Towers Watson SA/NV, Quai des Venes, 4020, Liège, Belgium (0415.981.986 RPM Liège) (registered as a branch in the UK at 51 Lime Street, London, EC3M 7DQ UK Branch Number BR021056) in relation to all EEA-regulated business. Authorised by the Financial Services and Markets Authority (FSMA) Belgium, and authorised and subject to limited regulation by the Financial Conduct Authority. Details about the extent of our authorisation and regulation by the Financial Conduct Authority are available from us on request

For further authorisation and regulatory details about our Willis Towers Watson legal entities, operating in your country, please refer to our Willis Towers Watson website. It is a regulatory requirement for us to consider our local licensing requirements prior to establishing any contractual agreement with our clients.

This newsletter offers a general overview of its subject matter. It does not necessarily address every aspect of its subject or every product available in the market. It is not intended to be, and should not be, used to replace specific advice relating to individual situations and we do not offer, and this should not be seen as, legal, accounting or tax advice. If you intend to take any action or make any decision on the basis of the content of this publication you should first seek specific advice from an appropriate professional. Some of the information in this publication may be compiled from third party sources we consider to be reliable, however we do not guarantee and are not responsible for the accuracy of such. The views expressed are not necessarily those of Willis Towers Watson. Copyright Willis Limited 2021. All rights reserved.