StrategicRISK

GUIDE TO:

People risk

SUPPORTED BY

D&O insurance solutions from AIG.

Today's directors and officers face more risk than ever, due to a growing breadth of regulations and heightened enforcement. Having the right coverage is critical. At AIG, we offer cutting-edge insurance solutions built to meet the challenges of D&O risk today—and will keep innovating to meet the challenges of tomorrow.
Learn more at **www.aig.com**

AIG®

Bring on tomorrow®

CONTENTS

Editor-in-chief Mike Jones
Editor Kin Ly
Assistant editor Ilonka Oudenampsen
Asia editor Jessica Reid
Executive editor, Asia-Pacific Sean Mooney
Head of sales Andrew Stone
Commercial director, Asia Pacific Adam Jordon
Senior production controller Alec Linley

Senior data analyst Fayez Shriwardhankar
Publisher Jack Grocott
Publishing manager Tom Byford
Executive publisher, Asia-Pacific William Sanders
Managing director Tim Whitehouse

Taking responsibility

The performance of staff, and particularly their integrity and professionalism, can determine whether a company stands or falls

AS A COMPANY IS only as strong and competitive as its employees, it stands to reason that businesses must look after their staff. This is not only because it is the right thing to do as an employer, but because its brand and reputation rests on them, their actions and the way they conduct business relationships.

If staff feel as though they are looked after, they will work better and be better advocates for their company's brand. If not, they are more likely to cut corners, take risks and start looking for another job. Human risk in its broadest sense covers both the wellbeing of staff and the wellbeing of the company.

As such, there is a fantastic opportunity for risk managers to partner up with their human resources (HR) colleagues.

HR and risk managers need to discuss a multitude of risks. These range from the health and safety of staff, including travellers and international employees, to attracting and retaining talent (where employee benefits schemes play an active role) and ethics, culture and behaviour.

Across these risks, D&O obligations now act as a driver to improving responsibility at board level, but employees are also growing increasingly aware of their obligations. They too have a duty – a duty of loyalty. This relates to their responsibility to behave and work with ethical integrity.

This joint responsibility – employers for employees, and employees for their employers – is why developing the correct organisational culture is perhaps the single most important part of managing human risk.

Indeed, culture plays a pivotal role here. But on a multinational level, compliance to core company ethics and D&O programmes is more and more difficult to manage: several jurisdictions now require the issuance of a local policy and/or a local premium allocation.

In this environment, insurance is an efficient part of the risk mitigation strategy, but it needs to be the right insurance. Companies must ensure they have the policy that is compliant across the world and in every market they operate in, or may operate in soon.

They also need the kind of global footprint that a multinational insurer can provide. These insurers have local offices across the world, with the capabilities to write policies in-country and draw on

'Organisations are reviewing their global mobility strategy and redesigning the programme elements, including policies, processes, technology, vendors and people'

Andrew Robb, Deloitte

reserves of in-depth local knowledge.

But a major problem for many firms is that they have grown faster than the infrastructure they have in place to provide duty of care.

"It is this pace of growth that poses the biggest risk to businesses as they sometimes fail to develop the security support functions that may legally be required of them, and which would ensure workforce safety and duty of care compliance," says Geoffrey Deane, business security director at Deloitte.

Greater diversity

Andrew Robb, global mobility, talent and rewards partner at Deloitte, argues that, in addition to an increase in the volume of assignments requiring staff to travel overseas, these assignments have also grown in diversity and range from commutes, permanent transfers, short-term business travel, project work, developmental assignments and rotators.

"This means more is being demanded from the global mobility professional and the programme support model, which was historically established to support traditional long and short-term assignments," he says.

"Organisations that are considered best-in-class in this space (only 8% of organisations, according to a recent Deloitte survey) are therefore increasingly reviewing their global mobility strategy and redesigning the programme elements, including policies, processes, technology, governance, vendors and people.

"This is done to ensure each component supports the overall business and talent objectives in an ever-more complex regulatory world."

Deane points out that the flow of information to and from an organisation's head office is vital when managing a large pool of mobile staff.

"Lack of up-to-date knowledge about employee locations, contact details and staff movements, when combined with an inability to adequately risk assess locations, develop/implement appropriate contingency plans and then advise staff, is unacceptable."

These risks can be mitigated by reviewing organisational structures to ensure any legal exposure is reduced. "One solution could be the establishment of separate legal entities," says Deane.

"A strategic-level approach can be further enhanced by creating appropriate roles/departments that are responsible for monitoring employees' locations, creating adequate emergency processes and collating all relevant intelligence. This can then be used to advise the business and employees on threats.

"Only then can a global entity ensure that their duty of care is appropriately discharged." **SR**

The opportunity of analytics

Increasing amounts of data are giving companies the opportunity to model staff trends more efficiently

THE AMOUNT OF DATA generated by businesses about their employees has increased massively, and one of the most promising areas of potential collaboration between risk managers and human resources is around the use of analytics and Big Data.

"We all do a lot of work gathering employee opinions through surveys, but how many firms really interrogate the data to get genuine insights?" says Yves Duhaldeborde, director, talent and rewards at Willis Towers Watson. "I'm very interested in the way we can use Big Data and analytics to make sense of our data and its effects on risk. Talent management and human capital are obvious areas where this approach can really help.

"As an example, I was talking to an employee who has just joined us and it struck me: if his previous employer had understood his background better, his ambitions, where he was in his career, what training he had – or hadn't – had, then he wouldn't necessarily have left that company to work for us." Recruitment and replacing talent has cost implications for businesses, he adds.

"If HR and risk managers look at these factors, then they can begin to model the likelihood of an individual leaving at particular points in their career. They might find that training on a particular topic after an individual joins a firm might mean companies are more likely to retain talent for another two years, for example. But this isn't done."

Generally, a firm might know what training an employee is getting and how their salary is progressing – businesses are, after all, capturing that data in one form or another. The problem is that they are not modelling it. "Companies are not working the data and using analytical tools to really interrogate this information, nor are they using that intelligence to make decisions," says Duhaldeborde.

Analytics has widespread applications across managing human risk, particularly in health and safety. Many companies »

'When one unit's safety arrangements were looked at in detail, it became clear that there was a serious risk of death'

Yves Duhaldeborde, Willis Towers Watson

» have gone to great efforts to develop their safety culture, of course. But establishing how successful they have been can be difficult. What needs to be done beyond standard risk management is using analytical tools to extrapolate what this information can tell a firm about its working practices and operations. Can businesses better predict when an accident or safety issue is likely to occur, for example?

"When one of my clients took the data gathered through staff surveys and ran it through a series of analytical tools, they were able to find out that one particular unit was very unhappy about their safety arrangements," says Duhaldeborde.

"When this was looked at in more detail, it became clear that there was a serious risk of death in this unit because its safety culture had developed to such an extent that its safety procedures were no longer viable."

Having learned this, risk management and human resources were able to work together to remedy the situation.

"By sharing information across functions openly, these units were able to identify trends that they may well have missed individually," says Duhaldeborde. "This is about active listening."

He adds: "There is a need for close collaboration, not only to anticipate problems, but also to develop the culture of the company and find values that will help eliminate risk, particularly reputational risk."

Technically advanced

This approach has been made possible thanks to recent technical developments and advances in analytics tools. "Take the example of large organisations with hundreds of employees across many countries," says Duhaldeborde.

"In the past, the kind of qualitative comments that these businesses would get back from staff surveys were very hard to analyse." They may have been in different languages or in the form of long pieces of text. Numerical analytical tools did not have much to offer a decade ago. "But now, there are tools that enable leaders to access data in a meaningful way and find patterns that provide real insight into how employees are feeling and how this varies across the organisation," says Duhaldeborde.

"For example, if groups of employees have lost their way on values, companies

'They can profile individuals, identify those thinking of leaving and ask: Why? What is it that they are not happy about?'

Yves Duhaldeborde, Willis Towers Watson

can spot that, address it and again, human resources and risk management can work together more successfully than they could on their own.

"They can also start to profile individuals, identify those thinking of leaving and ask: 'Why? What is it that these employees are not happy about and why do they have their CV out there?'"

These tools make action possible. They can identify problems with productivity and provide the means to discuss the why: do staff need training or better equipment? "Businesses can find these things out early, before the problems become critical, and do something about it," says Duhaldeborde.

"Take, for example, a building project that requires certain skills and there is a pool of people to whom the project can be allocated. All too often, companies don't carry out sufficient work to match the skills to the clients' needs. It may be that the client requires a certain amount of diversity, for example. These analytical tools help companies deliver what is required and do more for their clients, which is a very positive thing to be able to offer."

Analytics can also address future human risks that organisations may struggle with, such as workforce planning. Questions about the shape of a business, where it wants to be in the future and how it can be more sustainable can be answered. An action plan for challenges such as workforce diversity can also be developed.

"With this kind of information, not only can risk managers act with the benefit of expert help from human resources, but human resources can also draw on the experience of the risk department and get them to talk to staff and bring their perspective into day-to-day operations," says Duhaldeborde.

"People are really keen to see an end to silo mentality and this is a really positive way of achieving this and helping the company to function in a much more collaborative way." **SR**

Managing people risks

Understand your culture and you stand a better chance of managing risk to your human capital

Your people are your business and failing to manage this properly is a serious risk for companies of all sizes. Here, Simon Constance (pictured), people advisory services partner at EY and John Marsh, director of talent and people advisory at EY, look at the issues in detail.

Q. How does mismanaging human capital present a risk to a business?

EY: People and the culture of an organisation are critical to robust risk management, particularly in terms of risk ownership, identification, escalation and mitigation. We know that culture provides the norms of behaviour and failure, helping businesses to take into account how the organisation's culture will affect the ability to identify, understand and act on organisational risks. For example, a culture of fear or blame will inhibit critical risk escalation, which could prevent timely decision-making and corrective mitigating actions or effective continuity planning.

Mismanagement of human capital can occur for a number of reasons, the most fundamental being a mismatch of expectations between employee and employer. In addition, a breakdown in the 'psychological contract' could be a problem.

Although remuneration may be a key reason why people join an organisation, how employees are treated, often relative to others, drives performance and behaviour.

Finally, the work environment is also a factor in managing human capital. This extends to utilisation of human capital, and poorly managed shift planning, for example, can lead to higher absences and reduced productivity.

'Although remuneration may be a key reason why people join an organisation, how employees are treated drives performance'

Q. Are human capital risks increasing as firms become more complex and more global?

EY: Large and diverse companies will have a number of different cultures even without the additional complexity imposed through multinational

territorial cultural differences. The failure to account for these in terms of risk control design and implementation will limit a company's effectiveness and robustness. For example, does the culture support a rules-based or a principles-based control approach?

The risks are potentially greater with more complex supply chains. Although firms might previously have delivered their objectives through their own employees, this is rarely the case now. Most organisations are reliant on outsourced services and contractors. Having long supply chains undoubtedly presents risks to organisations and it is crucial that the risk from mismanagement of human capital is also managed in the supply chain.

Q. What can be done to better mitigate human risk? Does the correct approach differ from sector to sector or across departments and is there a gold standard?

EY: It important to understand whether there is organisational alignment on values, behaviours and purpose, within both the organisation and specific teams where risk is greater – for example in supply chains, people operating within the financial control framework and health and safety. The level of risk is dependent on company size, sector, shape and complexity.

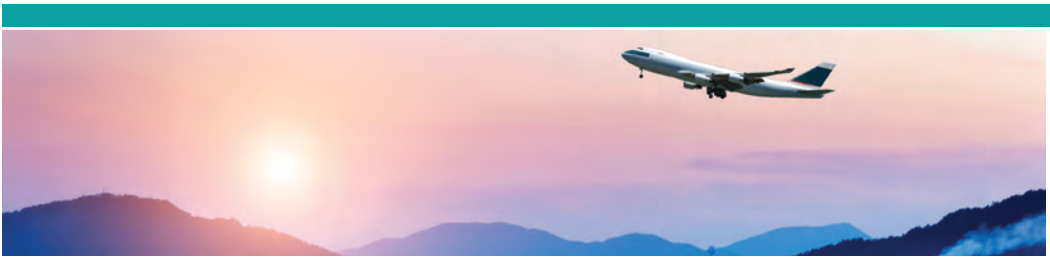
Also, incidents or regulation controls can, over time, build up in a way that creates a complicated, hard-to-understand control framework.

A lack of clear accountability and ownership of key risk controls could lead to a degree of disempowerment and disengagement, especially in environments that favour a principles or values-based control environment.

So in essence, an understanding of organisational culture informs the following: risk mitigation action, risk control design and implementation and the level of second and third-line oversight.

If organisational culture is not correct, then behavioural or values-based transformation may be required to mitigate the risk brought in by having the wrong culture, values and behaviour.

In other words, culture trumps compliance or controls. **SR**



Taking care of business

Employers have a responsibility to ensure their expat staff and families stay healthy, productive and safe

FAST-MOVING COMPANIES ARE THINKING globally and deploying their best talent to new operations across the world. In fact, the number of expat workers has grown more than ever before and is likely to increase.

"Although we have seen a reduction in 'traditional' assignments in recent years, there are more internationally mobile employees than ever before," says Marc Burrows, an expert on global mobility advisory services and a partner at KPMG.

With this comes complex duty-of-care obligations and care packages. But an off-the-shelf, one-size-fits-all care package is no longer fit for purpose, if it ever was. What an oil and gas business operating in Libya wants will differ from what an SME with operations in Singapore wants.

Operating successfully across diverse environments requires strong central control. "Companies don't like local subsidiaries organising their own insurance cover," says Marc Lenchant, AIG multinational manager, Europe. "Local knowledge needs to come on a multinational platform. It's not just about fairness of treatment or equality of treatment globally, it's also about cost control. If you know what you're providing centrally, you know that your duty of care is taken care of. But if you're allowing local policies to be given, and local healthcare, you open yourself up to problems about whether the best care is being provided."

This is especially true as companies now need to manage global mobility programmes that cater for many types of expatriates, from business travellers and cross-border commuters to global nomads and individuals working regularly across various locations. "Meeting the coverage needs of these employees with complex work patterns is a new challenge for companies, and insurance providers will need to respond to this by capturing new requirements into their standard policies, without compromising on price or global consistency," says Burrows.

Central oversight

But while a multinational firm is the best place to find cover, this needs to be more nuanced and adaptive than ever before. For example, there is a trend towards categorisation of location – hardship versus non-hardship – rather than simply looking at geography, which

'With companies in high-risk locations, the trend is to handle emergencies such as evacuations in-house at a company level'

Marc Burrows, KPMG

makes it easier for companies to ensure sufficient coverage while maintaining global consistency, and without overcomplicating the choice of policies.

"Companies usually have a suite of international assignment policies, offering different benefits depending on the assignee population and type of assignment," says Burrows. "But health and risk cover are 'core' benefits provided to all, so coverage is usually applied consistently without variation across division or segment.

"With companies in high-risk or dangerous locations, the trend is to handle emergencies such as evacuations in-house at a company level, rather than through individual policies with insurance providers. In this area of coverage, flawless execution of evacuation and other emergency services takes priority over cost."

Taking the global view means teams can think more strategically, spending more time on workforce planning, assignment structuring and talent development. "This, coupled with streamlining of processes and pressure to offshore or outsource administrative

THE RIGHT HEALTHCARE PLAN

With more people working overseas than ever before, businesses are facing greater challenges in terms of keeping employees – and their families – safe in sometimes difficult environments. A key consideration for employers is making sure they are sufficiently covering the medical risk posed by sending people into environments that do not have a British-style healthcare system.

"Relocating staff, even for a short period, is expensive and companies want to do all they can to ensure staff stay healthy, content and productive," says Claire Kenny, partnership manager, expatriate care at AIG.

"For this reason they want to ensure that their workforce are properly covered if they fall ill, but are also covered for routine healthcare and ongoing preventative screening, well-woman screening and child vaccinations.

"There is also a lot of interest in telemedicine, such as virtual clinics and services that enable staff to get in touch with a doctor or nurse who speak their native language via their mobile devices while in the office."

There is a focus on maintaining staff 'wellness' also, including services that address issues like stress, mental health problems and alcohol dependency, says Kenny. "One of the major reasons why expat operations 'fail' is because either the employee or their family, or both, do not settle in the new location.

"Companies often carry out pre-travel medical screening and some assess the health impact of a family's suitability for certain overseas locations: are expats and the families adequately prepared and resilient enough to cope with relocation?"

'There needs to be a clear differentiation of roles, so that nothing falls between the cracks'

Marc Lenchant, AIG

»

THE BROKER'S VIEW

A number of issues face employers managing their expat human risk. According to Adam Harding, international business development manager at Jelf, the key ones are security and health and wellbeing, not just in the traditional sense but in ensuring employees feel safe.

"More countries are looking to encourage new business set-ups in their regions and companies are looking to diversify their business risk and exposure by entering different markets. It is therefore key that businesses take the right approach to their expatriate populations," he says.

"It is vital for companies to use an experienced broker who is well versed in international markets and who has a good network of partners."

Each country has regulations for employee benefits and commercial insurances. Not meeting these can lead to fines or being excluded from doing business. "Research and preparation is important for a business to not only ensure they are set up compliantly, but also in ensuring that they have the right processes, procedures and policies in place," says Harding.

"For example, having the right international policy can really provide peace of mind for an employee and their family and help an expat assignment succeed. Without the right consultation from an insurance broker or intermediary, companies could end up taking out policies that do not cover costs for some eventualities in a particular region. In Singapore, for example, a routine maternity package can cost as much as £15,000 [considerably higher than some countries]."

Each insurer has different strengths in different regions, so it is important to choose one whose networks complement a company's expatriate footprint. "A broker is key in helping to guide clients to the available and suitable options for an insurance policy. Insurers need to ensure they work proactively and efficiently for clients, as the global market is never as straightforward as the domestic market," says Harding.

» work, means that companies want to spend less time on the day-to-day administration of policies and managing vendors, but without losing central oversight," says Burrows.

"Tools like dashboard cost reporting and central approval for exceptions are very popular with global mobility teams who have less time to spend on core mobility work, but no less responsibility, than they did in the past."

Of course, it isn't all about providing cover when things go wrong. According to Lyn Webb, senior manager, audit advisory at Deloitte, organisations are increasingly seeing the value of embedding risk management into travel plans for their employees. This can be as simple as actively sending area risk assessments to them when booking travel, often sourced from the Foreign & Commonwealth Office (FCO) website.

"Understanding the threats associated with specific locations requires more investment and some organisations see the benefit of this. By signing up to a managed service that provides HR or security teams with alerts, their threat awareness can be more agile," she says.

"Another growing trend is the employment of executive protection teams. This is no longer the preserve of high-profile political figures and royalty, as many senior business travellers employ executive protection, especially when business travel takes them across

challenging geographical borders. In terms of support to employees abroad, organisations frequently subscribe to app-based crisis communications plans, allowing both the traveling business person and their families to feel supported."

Working together

Again, it is important that these additional services are provided at a global level with appropriate controls. "There needs to be a clear differentiation of roles, so that nothing falls between the cracks," says Lenchant. "The risk department is often more about risk and physical assets rather than individuals, while the HR people are worried about recruitment, training and the physical wellbeing of people.

"Neither one has got it fully in their remit and they need to make sure they are working together in a responsive way. Only then can they be sure that they are meeting their duty of care." **SR**

BEST PRACTICE: WHAT TO PROVIDE

Before departure

- Online security awareness training for employees
- Country reports to inform staff and advice on what precautions to take
- Global news watch emails

When travelling

- Travel assistance and concierge service
- Security travel alerts, for example SMS and email security news
- Translation tools and resources

Anytime services

- Health portal – remote nursing services
- Medical second opinion

THE BENEFITS OF MULTINATIONAL COVER

- Local claims – a timely and efficient claims service in local languages
- Service excellence – a centralised point of contact with one underwriter/carrier for a global programme
- Multinational flexibility – option of master policies with DIC/DIL coverage
- Local servicing – local language certificates and local assistance
- Coverage control – standardized coverage terms and conditions across affiliates and subsidiaries

Road worthy

Companies are legally obliged to ensure that their employees are as safe as possible when on the road doing business on behalf of the firm

ALL COMPANIES HAVE A duty of care to their staff and failure to ensure this can have disastrous consequences. But in the modern, globalised business world, making sure your employees are safe requires detailed understanding of how regulations work across borders – and what's at stake when things go wrong everywhere you operate.

For example, in Europe the concept of a duty of care owed by an employer to its workers is now a central part of the Health and Safety laws of EU Member States. "As such, there are now powerful legal, reputational and commercial considerations compelling organisations to acknowledge and discharge a duty of care to employees sent abroad on the employer's business," says Teresa Hitchcock, partner in the litigation and regulation practice group at DLA Piper. "These will be particularly cogent where the cross-border assignment is to a country with limited health and safety legislation, or enforcement, or where security is an issue, and ultimately is requiring businesses to engage actively by imposing internal risk management procedures."

This is likely to apply wherever in the EU employees – and their families – have been sent. But while some criminal or regulatory aspects of health and safety legislation only apply in certain member states – and an incident outside its borders will not then result in proceedings in that country – other obligations under general criminal law may apply on a cross-border basis.

A good example is the UK where, although the Health & Safety at Work etc Act 1974 (HSWA) only has legal effect within Great Britain and on certain offshore installations and pipelines, the reality of its application is more complex. "It should be noted that many of the duties under HSWA will be breached in the event of the exposure of a person to a risk, and it is not necessary to show that an injury has been caused as a result," says Hitchcock.

"Therefore, an employer may well be potentially liable in Great Britain for a failure to conduct a suitable and sufficient prior risk assessment in respect of risks to an employee who has been posted abroad. Also, it should be pointed out that incidents involving employees posted abroad may incur liability under the law of the country to which the employee has been posted."

'Documentation of risks assessed and measures taken to mitigate them are essential'

Teresa Hitchcock, DLA Piper

Getting it right

Potential penalties under the HSWA include an unlimited fine and imprisonment. Because of this, firms need to make sure they get it right. Staff need to be trained – and that training documented – they need refreshers where necessary and they need adequate support in country. There also needs to be ongoing risk assessment that addresses any particular hazards. "As always with health and safety legislation, it is not sufficient to »

» merely comply, the organisation must also be in a position to prove that it has complied," says Hitchcock. "Adequate documentation of risks assessed and measures taken to mitigate them is therefore essential."

The right insurance is also essential and employers need to make sure they choose cover that has the power to react effectively and at a speed and scale commensurate with any given emergency [see box]. It is worth remembering that this is not just about defence. Getting duty of care right is also an opportunity to project a powerful message about how good you are as an employer.

This is important because when things do go wrong and a firm fails to deliver on duty of care, the impact can go beyond the incident itself – and legal action is not all a firm risks. "There can be bad publicity, reputational damage and an incident can send ripples throughout a company," says Jonathan Lord, lecturer in human resource management and employment law at Salford Business School. "There can be resentment created between local and expat workers or different teams if there's perceived injustice, and this can create ongoing rifts."

In the end, this is about individual wellbeing – and corporate wellbeing – and no one can afford to be caught napping. **SR**

DUTY OF CARE: GETTING IT RIGHT IN NEPAL

Within hours of Nepal's devastating earthquake in 2015, AIG Travel initiated a detailed plan to provide security support, evacuations and humanitarian aid to more than 100 AIG clients. This included security information, medical consultations and other assistance services around the clock.

A crisis management team was sent to the region and was on the ground within 48 hours to help begin client evacuations in Kathmandu and more remote areas of Nepal, including helicopter evacuation from Mount Everest. Medical assistance was provided to everyone who needed it. Food and supply drops were also made to clients in remote locations who were running low on critical supplies.

A 737 airliner was chartered to get expat AIG clients to Delhi and all crisis response operational activities in Nepal were completed within six days of the start of the operation.

BUSINESS TRAVEL BEST PRACTICE CHECKLIST

1. Increase awareness of risk
2. Plan with key stakeholders
3. Expand policies and procedures
4. Conduct due diligence
5. Assess risk prior to every employee trip
6. Communicate, educate and train
7. Track travelling employees at all times
8. Implement an employee emergency response system

STAYING HEALTHY OVERSEAS

When creating a medical travel plan, it is important that risk managers go through every stage of a systematic approach.
1. There needs to be appropriate training and advice for the traveller pre-trip.
2. The organisation should have a process that enables it to locate travellers in the event of an emergency (travel tracking)
3. While abroad, the traveller needs to have access to good levels of support. This could be telephone access to medical staff, but it also means appropriate access to someone with emergency skills and good awareness of the location.
4. Health and safety onsite is particularly important as trips and falls can be a major source of medical problems.
5. There is also a lot that can be done onsite to make medical conditions better. For example, malaria eradication programmes and health education of staff, including sexual health and hygiene.

APPROPRIATE INSURANCE

Having the right insurance in place is vital as business travellers are exposed to a wide range of risks, from lost luggage and lost data to injury, arrest, kidnapping and medical emergencies. A global provider such as AIG can assist business travellers through both multinational programmes and local knowledge, along with its raft of integrated people risk insurance covers and unparalleled global security network.

"The type of policy that a company goes for depends on what you are looking for but, broadly speaking, clients are driven by three facts, all equally valid," says Linda Beavis, principal consultant at Aon Hewitt. "Some are focused on ensuring staff are at least as well covered as they are in the UK, some are focused on being compliant and others are looking at cost and want the most economical policy.

"There is no one-size-fits-all approach and different companies, sectors and variations in corporate culture all need to be taken into account."

On dangerous ground

Expanding trade into uncharted markets and often hostile regions can bring with it an increasing threat to employees

ALTHOUGH KIDNAPPING HAS BEEN a risk for years, recently – with the spread of ISIS – there has been a shift from hostage-taking for ransom towards more brutal attacks, motivated by the desire to terrorise and secure political concessions.

"For many, this is very hard to understand and harder still to counter," says Jon Gregory, global head of kidnap & ransom (K&R) at AIG.

"What we expect to see in the near future is a continuation of the trends we have seen for the last three or four years, which stem from the emergence of a loosely-defined terrorist caliphate from Afghanistan through the Middle East and down to the northern sections of Africa.

"The issue for insurers is that hitherto, K&R threat has been more restricted geographically and kept largely away from areas where commercial businesses

operated. We used to see clients looking for cover principally because of commercial operations in South America and, while that still prevails, it does not drive sales in the capacity it used to and a lot of the conversations we have now are not focused solely on this geography."

"Preventing this more sinister style of kidnapping is very difficult," says Paul Mills, global prevention manager at AIG Global Security. "As we have all seen, it can end badly. In addition, government regulations to prevent the funding of terrorist groups influences the ability of firms to pay ransoms. The usual mechanism of negotiation and release is not present and this represents a serious challenge to the industry model."

Unstable places

This situation is further complicated by economic changes and the search for new markets. Driven by a European recession and the subsequent need for growth, corporates have been expanding into emerging markets. Simply put, there are more people in more unstable places.

"We have to accept the fact we have a lot of clients with interests in these difficult environments and work with them on that basis," says Gregory.

"Increasingly, there is exposure in environments that would have previously been considered very safe. We need to help educate people about these changes."

This means that firms with no real history of addressing K&R and security risks on this level are placing staff in dangerous situations, often without realising what is at stake.

'Some small non-governmental agencies are fantastically well informed, but we see large multinationals making some pretty naive assumptions'

Alex Kemp, NYA International

"Until recently, these places were primarily just a source of natural resources for export," says Julien Monegier du Sorbier, head of kidnap and ransom, EMEA at AIG. "Now they are part of a global economy, attracting a whole new spectrum of commercially interested parties, not simply limited to large multinationals. These new operators, due to their smaller stature, are often much less prepared for the risk inherent to these locations and lack the necessary experience and resources to manage them.

"They often go to these places without appropriate comprehension of the risk and therefore may ignore the complexity and variety of the threat to their resources and business. In reality, the risk tends to be the same for a large multinational or an SME. You will be seen as a Westerner and therefore a target." »

» According to Alex Kemp, managing director of crisis prevention and response firm NYA International, all companies should give this issue some thought: "Risks vary for different organisations, including the nature of activity being undertaken, geography, profile and preparedness; however both large multinationals and SMEs are targeted. This can be a particular problem for SMEs that are contracted to work for global companies in their supply chain. Unlike the multinationals they are partnered with, these firms may not have appropriate experience to operate in these environments or even really understand that their staff could be subject to K&R."

He adds: "The threat [landscape] has changed so much. Not only can terrorists strike in any market, but firms may be affected indirectly by an attack and face business interruption problems as a result," he says. "Sadly, over the next few years, there will be more attacks by lone wolves or small cells and these will only go to further focus people's minds on the risk."

The groundswell is building

In this environment, every firm needs to take responsibility for security risk and more are doing so. "So far, there is a gradual take-up [of security responsibility] but the groundswell is building with every incident," says Kemp. "An awareness of terror is becoming the new normal."

In many cases, it is employees driving this change. "Terrorism is increasingly a factor employees consider when they make day-to-day decisions," says Kemp. "I know people where I live in Scotland who have cancelled trips to London because they are worried about attacks. Because of this perception, employees expect their employers to do all they can to protect them."

Multinationals will probably have a dedicated security team but in smaller firms, security will probably be dealt with by human resources. "When we talk to firms, we see a hugely varied level of awareness," says Gregory.

"Some small non-governmental organisations (NGOs) are fantastically well-informed, but we see large multinationals making some pretty naive assumptions and risk management practices. A lot of this comes down to industry sector. If NGOs and those working in oil and gas didn't have robust procedures and flexible plans, they wouldn't survive. They have to know how to keep secure and get their people out in an emergency. But they also need to know how to continue to operate. They can't abandon a location. They have to be tough."

All firms operating in dangerous environments have something to learn from this attitude and need to develop their corporate governance duty of care accordingly. Simply put, they need to beef up their focus on people risk management.

"This is the only way to fight back against the terrorists and help prevent employees becoming puppets in a political play that unfolds in front of the world's press," says Mills.

Understanding context is key to doing this. AIG divides the world into three zones for K&R purposes: permissive environments, such as the UK; semi-permissive environments, such as Algeria; and non-permissive

'Things go wrong when management finds itself too remote and distanced from what is actually happening on the ground'

Paul Mills, AIG

environments, including Syria and Yemen. These definitions are then used to shape the level of risk management needed. In permissive environments, there need to be good security and safety procedures, but these can operate in the background.

In a semi-permissive environment, there will be more day-to-day support, infrastructure, training and a substantial security focus. In non-permissive environments, there needs to be extensive training and a substantial security presence, possibly including armed guards and armoured vehicles.

"There is huge granularity in terms of the service we offer," says Mills. "We have developed a plan to give clients a real, tangible understanding of their risk, context by context.

"We have to constantly innovate and design solutions specifically for clients. These can go a long way towards eliminating K&R threats. We help select the best people, provide a fantastic level of support and build around that an infrastructure that is robust and capable of responding quickly and effectively.

"Things go wrong when management finds itself too remote and distanced from what is actually happening on the ground. Everyone in the chain needs to understand what is going on at the coalface and we help to ensure that's happening."

Complacency is a real danger. "People going into non-permissive environments know they're very dangerous and take precautions," says Mills. "What worries me more is people going into the semi-permissive environments and feeling isolated."

Going it alone

These days, the real risk is likely to be to a businessman going alone to the likes of Algeria without any infrastructure around them, staying in a normal hotel and taking local taxis. "In any line of insurance, liability is becoming increasingly important. There are several examples where employees have been caught up in kidnap and ransom events where, upon resolution, said employees or their families then sued their employers for a failure of duty of care," says Monegier du Sorbier. "If an incident is badly managed, it can cost the company."

But the risk management support associated with good insurance can help close that skills gap and make sure employees are aware of the risk. They know how to travel, how to act, and how to stay safe. "Plus," says Mills, "if the worst happens, we will make sure businesses have the right crisis management team in place with the resources that it needs to ensure companies get the best possible outcome." **SR**

Staying ahead of the pack

As the scope of terrorism attacks widens, companies are having to keep up with the complexity of threats to staff

THE RISE OF ISIS and the increasing brutality associated with its actions are shifting the focus of insurance, away from the cover available after the event to the risk management available to help prevent an attack taking place. "One of the things we are trying to do is put more services behind the product," says Paul Mills, global prevention manager, AIG Global Security. "Most clients increasingly say to us that what they want from the product is less the indemnity and more the service behind that, we want to respond to that need.

"We need to be there from the start to help them protect their staff and develop the capacity to remove people from an environment in a hurry if the situation deteriorates.

"These are certainly interesting times. The dynamic of these abductions has changed so much. In the old days, there was a progression that contained the assumption that this was a cash transaction; they were primarily interested in money.

"With Islamic groups, that has all changed. Because these groups have such a bold political ambition, their demands are often much harder to untangle and deliver. As we have seen many times, the results are often tragic.

"What we are trying to do is align our approach more broadly to people risk. Many other products cover risk to people and we need to ensure these operate seamlessly, so if we have a complex event that is across multiple products, we are able to work across silos to bring an effective solution."

Rex: AdrianHancu

The risk at home

The terrorist threat abroad is no longer the only scenario businesses need to consider when it comes to safeguarding their employees during work time.

As the attacks on the offices of Charlie Hebdo in January 2015 brutally illustrated, corporate property in the heart of Western Europe is also at risk.

"I have spoken to major media companies who are very concerned about this risk because they have had direct threats," says Mills.

"But when I go and visit their premises, I can see straight away that they are wide open to attack. Of course they are, because they are in a permissive environment, where staff are confident and open. That's a good thing. The challenge is in finding a way to address security concerns in this context."

For example, it is fairly typical for a firm's emergency plan to require staff to evacuate and find a rally point outside in the event of an incident. But this approach may need to be adapted in an event of an armed terrorist attack. Triggering an emergency plan that requires staff to regroup outside in a big crowd may be asking for trouble, if there are active shooters targeting corporates.

Mills adds that people tend to see K&R as about kidnap, "but increasingly it's about hostages. We are seeing more and more incidents where employees are being held against their will and these corporate-based hostage situations all have a call on the K&R policy that enables risk management in advance. Take advantage of it." **SR** »

DESIGNING A SECURITY PLAN

- Conduct a full risk assessment for every location, keep it constantly updated to reflect any changes on the ground – and make sure you use it as the basis for all risk management decisions.

- Training must be up to date – and regularly refreshed – to keep staff confident and effective in their work. Carry out regular scenario planning and test your responses.

- Ensure that you have an effective journey management programme that considers both locations and the routes between them. Use well-maintained vehicles, get the right drivers – and train them.

- Complacency is the enemy. Familiarity breeds contempt for procedure and firms must require staff to maintain an appropriate level of vigilance and carry out all necessary safety checks on an ongoing basis.

IF THE WORST HAPPENS

Risk managers can do a huge amount to lower the risk of a kidnap, but in the end we all have to face facts: it could still happen. What do you do then?

Speed of response is essential and if the worst happens, then everyone needs to know how to act.

First, there needs to be a dedicated emergency team with representatives available from across security, risk, travel and HR. It is also important to remember the communication and PR aspects of a crisis.

Teams need to have the skills and mandate to take control and manage events while the rest of the business carries on as usual.

To ensure this happens, there has to be a crisis management plan ready to go and this needs to be reviewed on an ongoing basis.

KIDNAP HOTSPOTS

LIBYA There has been an upsurge in kidnapping activity in the northern coastal regions carried out by criminal, extremist and militia groups, particularly around Benghazi and Tripoli.

SYRIA AND IRAQ In Iraq, the area of highest risk is in the central and northern Sunni areas. All areas of Syria are considered high risk.

AFGHANISTAN All areas considered high risk, especially southern and eastern areas.

PAKISTAN Risk of kidnap by both criminal and Islamist groups, particularly in the Khyber Pakhtunkhwa provinces, Karachi and the north western tribal areas.

NIGERIA AND CAMEROON Risk from both the Boko Haram insurgency and criminal groups.

SUDAN Kidnap remains a common tactic for militant and rebel groups, especially in Darfur.

YEMEN There are regular kidnappings of locals and foreign nationals by tribal, extremist and criminal groups.

SOMALIA AND KENYA Criminals and Islamist terrorists pose a risk particularly in Somalia's Galmudug and Puntland regions and along the Somalia-Kenya border.

THE SAHEL Weak border controls have allowed criminal and Islamist groups freedom of movement leading to a high kidnap risk, particularly in central and southern Algeria, Mauritania and northern Mali and, to a lesser extent, Chad and Niger.

MEXICO Criminal gangs continue to target locals and some foreigners, particularly in Tamaulipas, Michoacán, Guerrero, Tabasco and the Morelos states.

VENEZUELA Criminal gangs in collusion with corrupt police and officials continue to make Venezuela a very high-risk location.

PHILIPPINES AND MALAYSIA The threat is primarily from the Islamist group Abu Sayyaf and others in the Philippines' southern Mindanao region and the Sulu Archipelago, as well as Malaysia's Sabah state.

Making the most of new working practices

If applied shrewdly, flexible working arrangements can give companies a competitive advantage

ADVANCES IN TECHNOLOGY MEAN that employees no longer need to be on site to work and this has given rise to a raft of new working practices built around more flexible hours. With the introduction of recent legislation, 95% of employers now say they offer some form of flexible working.

However, some managers are resistant to flexible working. "These work arrangements continue to be perceived as concessions for individual employees, illustrating reduced commitment as opposed to a more efficient way of working," says Emma Stewart MBE, joint chief executive, Timewise.

These changes do not just offer employees new ways to earn their living while having a good work-life balance. By maximising the opportunities on offer, they enable firms to reduce staff turnover – a risk that is exacerbated if companies fail to adopt flexible work practices.

A survey by a UK mobile phone company, for example, found that 23% of its workforce would resign if they were not

'A more engaged culture means a more stable workforce'

John Hopper, AIG

offered flexible working arrangements. Conversely, in another survey by the Chartered Institute of Personnel and Development, 46% of British workers said they would take up more flexible work arrangements if it were offered to them.

Competitive edge

From an employer's point of view, recruiting is expensive and every time someone leaves, they take with them a piece of institutional intelligence. However, flexible work arrangements – and advertising it – will give businesses a competitive edge.

"Forward-thinking businesses who are able to understand and evaluate the specific job design, embracing flexible working practices from the point of hire, will be the employers who achieve a competitive advantage in attracting and retaining the best talent, translating into improved productivity and profitability," says Stewart.

"There are 14.1 million workers across the UK who are now looking for some form of flexibility in their next role," she adds. "By advertising roles with flexible working options, businesses across all sectors will be surprised as to how many more skilled and diverse candidates they will attract."

Flexible working also creates an open, engaged environment where employees

feel they can speak out and be heard has the dual benefit of creating happier employees and a more effective, profitable organisation.

"Achieving this may well demand an improvement in leadership skills to ensure that employees are able to develop and make the most of their skills and experience," says John Hopper, head of financial lines UK, AIG.

"A more engaged culture also means a more stable workforce. Most people don't just stay with an employer for the money, they need to feel valued and listened to as well, and that they have a future with the organisation.

"Creating an engaged culture is about making the most of what you have and designing an environment where people want to come to work. Benefits then flow through in terms of innovation, more focused training and, ultimately, enhanced profitability," says Hopper.

The right culture also reduces a company's risk profile in other areas. "A poor culture often means a riskier business," says Hopper.

"With an engaged workforce, regulation and compliance can become a positive benefit to the business as you have a culture of continuous improvement and a desire to be the best, both ethically and ultimately financially."

Engaged team

With an engaged team, risk management becomes a top-down and bottom-up conversation. "Risk management should not only be about risk managers creating structures and procedures that employees should adhere to," says Hopper, "but about establishing an environment characterised by an open and ongoing conversation that accurately reflects how an organisation functions and addresses its risk.

"In addition, an engaged workforce has social benefits that can impact risk improvement with much more likely awareness of staff issues involving drink, drugs or gambling, which all may impact risk management around theft or fraud."

Businesses also need to get their culture out there and talk about it. Risk managers should help their colleagues in human resources ensure a corporate culture is present in the recruitment process, and that they understand their role in risk management, as well as how a good corporate culture can affect their ability to deliver this.

"The key to maximising good corporate governance and risk management is to create a culture that engages all employees in the business, from the shop floor to the boardroom in the business process," says Hopper. **SR**

TYPES OF FLEXIBLE WORKING

- Part-time working
- Flexi-time
- Job-sharing
- Remote or homeworking
- Compressed hours – for example, fitting a five-day week into four days
- Term-time only working
- Flexible annual hours

When the enemy is within

Whether it's a stolen stapler or a series of illegal trades, companies need to address crime committed by their own staff proportionately

NO ONE LIKES TO think their own employees are stealing from them, but it is a fact that crime committed by staff is a major business risk. From stealing office supplies to making illegal trades, firms need to be aware of the threat.

But they need to address it intelligently without compromising their corporate culture with excessive security.

"The insider risk varies from organisation to organisation," says Angela Sasse, professor of human-centered technology at University College London. "In low-wage, high-turnover places, in which people don't see a career path, businesses will experience more insider fraud than in more professional organisations."

Generally, the problem can be divided into three areas: staff set out to defraud their employer; staff complacency makes it easier for other criminals to steal from or defraud the firm; and staff being blackmailed or otherwise manipulated into committing crimes. "Insider fraud can be a particularly emotional thing," says Sasse. "It's often quite uncomfortable to think that your own colleagues will act against you and so some firms will avoid the issue."

While the number of insider attacks may not be as high as those by external criminals, they tend to have a higher success rate and more of a financial and operational impact. "Particularly where employees are defrauding from inside the company, they often know how to cover their tracks and they can be hard to catch," says Sasse. "Some attacks can go on for years without being discovered."

But protecting the business is easier than many might think.

Saving their blushes

When frauds are investigated, it often turns out that the criminal has committed similar crimes in other companies, which could have been identified through better screening at the recruitment stage.

"Often a problem arises because a previous employer was embarrassed to have been caught out, and so they let people go quietly to save their blushes," says Sasse. "Thorough screening is important, particularly if businesses are recruiting to positions where staff have a lot of access to valuable material, money or sensitive data, or in businesses where working practice can be hard to monitor continuously. In these cases, there needs to be appropriate screening."

There also needs to be appropriate wording in employment contracts. "Psychological contracts [the perceptions of the two parties, employee and employer, of what their mutual obligations are towards each other] that explicitly point out that certain behaviours are forbidden, such as harassing or bullying colleagues, are becoming more common," says Sasse.

It is also critical to design your security system so that it actually works on a practical level and staff can comply without compromising their ability to do their job.

"Many attacks are carried out by disgruntled employees and often more work can be done to identify when workers are likely to fall out with their employers and thus become more likely to commit fraud," says Sasse. Businesses can (i) actively manage the problem and work to provide training or other opportunities to help mitigate the situation; or (ii) put a watching brief in place and monitor an individual or situation closely.

Monitoring IT networks is important, but it should not be relied upon too much. "Monitoring software could catch some very emotive people, but many will slip through the net," says Sasse. "It is also quite expensive to do continuously. A better approach is to have the capability to turn monitoring systems on when companies have intelligence to indicate that something is wrong. Continuous monitoring can also have a negative impact on staff, as most people don't enjoy the feeling that they are being constantly spied on."

Perhaps the single most significant step a firm can take to mitigate the risk is creating an open and engaging culture whereby staff value their workplace and treat each other with genuine respect.

Often, when there is an investigation after an attack, it turns out that co-workers were aware that their colleague was stealing or defrauding and were either too intimidated or apathetic to take any action.

"For this reason, it is vital for businesses to have some kind of no-fault reporting process in place to ensure staff feel comfortable to speak up if something is wrong – even if the crime involves their manager or if they are worried they might have made a mistake," says Sasse

Trying to do the right thing

Not all fraud by employees is deliberate and many may be the victims of fraud themselves. For example, the so-called 'fake presidents' scam involves criminals convincing an employee that they need to make an emergency bank transfer to a third party to fulfil some essential function, such as pay off a debt, service a provision in contract or make a deposit.

This type of scam is usually carried out by well-organised groups who carry out a great deal of research into market conditions, the structure and the customers of the companies they are attacking.

However, the central premise of the scam – a request by a senior member of staff – is often enough to coerce employees into action through fear of repercussions from disobeying authority.

According to experts at Deloitte, the criminals typically use persuasive dialogue such as: "It is an order to do this", "I count on you for your efficiency and discretion", and "The success of the project rests on your shoulders". The only way to prevent this kind of attack is through staff training that emphasises: these cons exist and staff need to be vigilant for anything unusual; always stick to established protocol around transfer; and always verify a request by using your own contact info, not those provided in an email. **SR**

'Monitoring software could catch some very emotive people but many will slip through the net'

Angela Sasse, University College London

Human risk: the real cyber threat

Employees being duped or blackmailed, or simply turning against their employers, are perfectly placed to help cyber criminals

CYBER RISK IS NO longer just an external threat. Disgruntled staff – or employees being blackmailed or otherwise pressurised – are now co-operating with criminals to carry out 80% of malicious cyber breaches from within, according to a new Knightsbridge Company Services (KCS) White Paper, *Cyber Matters: The threat to security in this century*.

As organised criminals forsake traditional methods such as armed robbery in favour of cyber crime, and the number of attacks multiplies, how can firms protect themselves?

Employees who are duped, blackmailed or who simply turn against their employers are perfectly placed to help the gangs.

Q. Are internal attacks a growing threat?

KCS: Organised criminal groups are becoming increasingly sophisticated in their use of social engineering through phishing and spear phishing methods. In practice, this means trawling social networking sites such as LinkedIn and Facebook to discover personal details about key employees. These can then be used to create phoney emails to other members of staff, in order to blag their way inside a system, such as asking them for personal log-in details so that they can 'confirm their details on their new database' or simply telling them to transfer some funds to an amended account.

Social engineering uses employees' own information against them. By trawling social networking sites, skilled hackers can accurately guess employees' passwords or narrow their brute force password software and make it more focused. Crucially, these are precisely the fields found in approximately 90% of passwords.

Without naming them, several of the latest hacking attacks aimed at Western commercial organisations, which resulted in massive data losses, were not caused by major hacking attackers using the ubiquitous denial of service attacks or by creating huge lines of code to access data through weaknesses in the company's cyber defence systems.

In fact, in one incident, hackers were engaged in an effective social engineering assault against a company's IT manager. The manager had created an admin login with access to everything so that he

could fix any problems himself. In doing so, he had given the hackers an easier way of discovering his simple password and they promptly used this log in to steal the company's data.

So the distinction between internal and external is blurred somewhat, but the most damaging data losses usually involve an internal source. Whether that person is aware of their role is usually debatable.

Q. Your research mentions the use of 'honey traps'. Are there other examples of how employees might be manipulated by criminals?

KCS: Staff should be aware that just because no one has approached them or spoken to them, it does not mean that sensitive corporate information has not been stolen. Public WiFi areas are now magnets for hackers as the technology needed to hack into users' systems when they are using public WiFi is available online for around $100. This rule applies even more to staff travelling in regions such as China, where cyber espionage has become a major state-sponsored industry.

KCS has initiated projects that used the same tactics as hackers. We set up a false-flag profile whereby a targeted approach was carried out on an audience of lawyers during a London conference.

We used a female profile [of a Czech purporting to be a senior manager at a law firm]. Of the 200 lawyers who attended, we targeted 100 within 48 hours. Of that 100, 50 had connected with Marina on LinkedIn (all those targeted were done so with the chairman's permission under strict secrecy and a confidentiality agreement).

From these LinkedIn connection requests, almost all had left open their connections so that 'Marina' could discover all of the target's business network connections. As you can imagine, that would also lay bare who their customers and clients were.

Because this was run under strict confidentiality with the chairman of the

'Technology to hack into users' systems when they are using public WiFi is available for around $100. In China, cyber espionage has become a major state-sponsored industry'

KCS

forum, when the connection happened we disconnected immediately. It was an example of 'if the hat fits…'

But this, of course, is just a start for criminals. In reality, hackers could then target victims on other social media platforms, collecting data to gain the target's passwords, opening up a whole world of trouble for the targeted person.

Q: You mention weaknesses brought about by the growth of BYOD, are there any other developments or changes that create weaknesses?

KCS: With BYOD, most users use hardware and software for home and business work. How to carry out compliance with the company's information assurance and security policy is, at best, extremely difficult. What is needed is a system that sets policy and enforces it automatically without the human element being able to break the rules. This service is an effective way of keeping company information assurance and business documents clean from malware.

Q. In cases of malicious attacks, how can HR and managers better prepare staff to minimise this risk?

KCS: The process is twofold and involves staff education combined with deployment of software, which automatically tracks any unauthorised or unusual activity, such as sensitive corporate data being illicitly uploaded on to a USB stick or any other external hardware. Any employee leaving the company has plenty of opportunity to take the company IP or documents without anyone knowing, unless there is a good security system in place.

Education through presentations and demonstrations would also encourage staff to grasp that internet security can only be achieved if staff understand that the weakest link in a company's cyber defence is themselves. **SR**

SUPPORTED BY

Beaded craftwork, South Africa – Where AIG insurers have done business since 1962

We understand that no two multinational businesses are alike.

Every organization has its own risk exposures and risk tolerance. At AIG, we'll work with you to help create a programme tailored to your specific needs, virtually anywhere you do business—whether that means local policies in some or all of the places you have exposure or a single global policy. Learn more at **www.AIG.com**

AIG®

Bring on tomorrow®