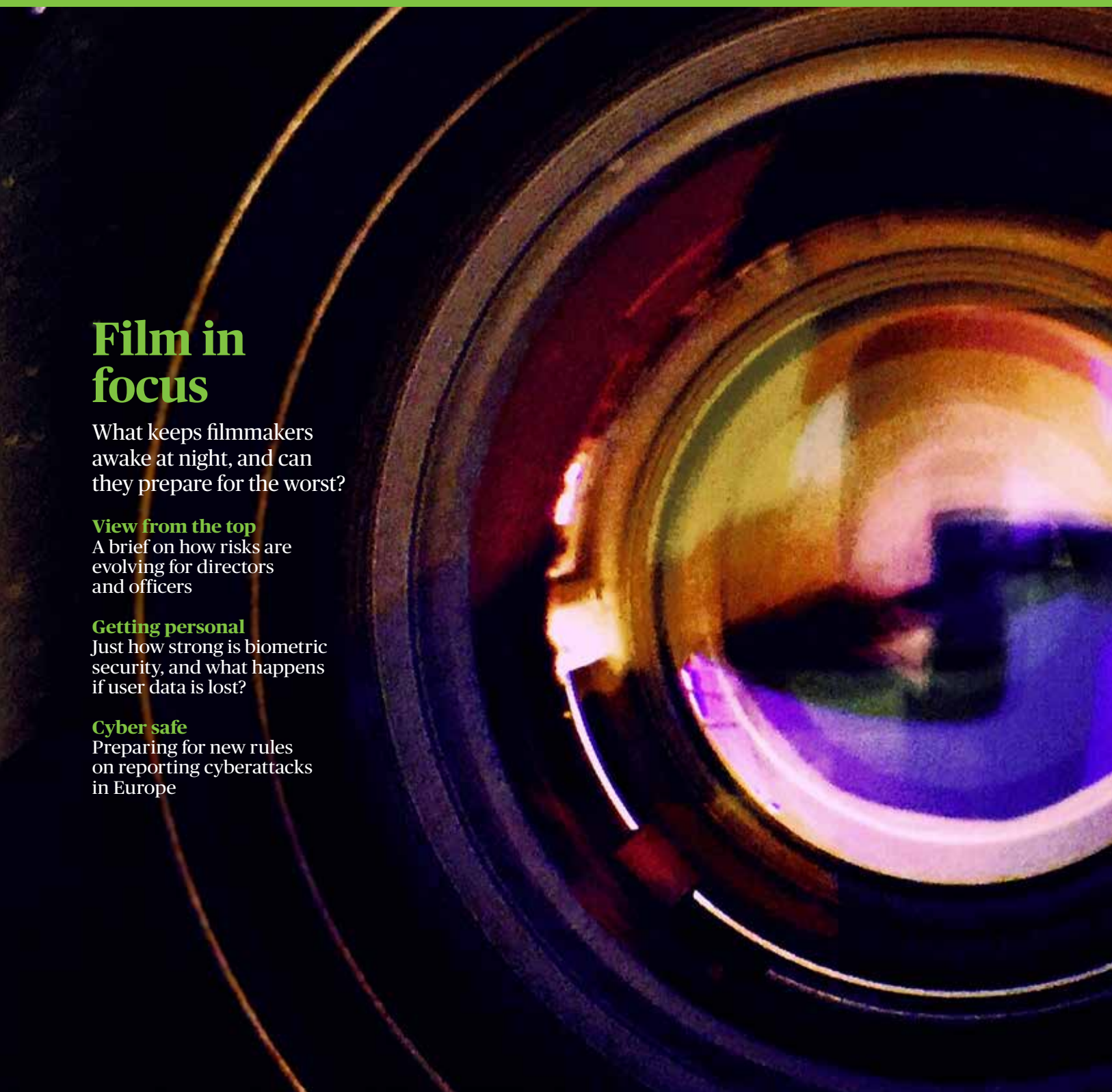
CHUBB®

2017 Issue 1

Progress



Film in focus

What keeps filmmakers awake at night, and can they prepare for the worst?

View from the top
A brief on how risks are evolving for directors and officers

Getting personal
Just how strong is biometric security, and what happens if user data is lost?

Cyber safe
Preparing for new rules on reporting cyberattacks in Europe

Welcome

In the light of recent and current events, change is on everyone's minds. It is also a recurring theme in this edition of *Progress*, which explores the evolving risks and new legislation that should be on your radar.

In the entertainment industry, where imagination is the only limit, no two projects are the same. But, as we learn on page 8, insurers are innovating to support filmmakers. Imagination is also at the disposal of criminals, who are finding novel ways to crack biometric security systems. With more companies deploying the convenient technology, we speak to a top hacker about how to stay ahead of fraudsters and find that regulation is evolving.

We also explore new regulation that directors and officers must comply with, and the cyber rules that will affect companies in essential sectors, such as banking, across the European Union from 2018.

On page 22, taking a step back to consider the place of risk managers within organisations, FERMA president Jo Willaert urges a leadership role.

I hope you enjoy reading *Progress* and find the insight of our interviewees helpful in mitigating risk.

Andrew Kendrick
Regional president, Europe
Chubb

CHUBB®

If you would like to discuss any of the issues raised in this publication, please contact Darragh Gray on +44 (0)20 7173 7578 or Valerie Gagnerot on +44 (0)20 7173 7585 or your local Chubb office.

ACE has acquired Chubb, creating a global insurance leader operating under the renowned Chubb name. ACE European Group Limited registered in England & Wales number 1112892 with registered office at 100 Leadenhall Street, London EC3A 3BP, authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

Additional information on Chubb can be found at www.chubb.com/uk

Progress is published on behalf of Chubb by Wardour, 5th Floor, Drury House,
34-43 Russell St, London WC2B 5HA
Tel +44 (0)20 7010 0999
www.wardour.co.uk

Editor Jane Douglas
Content Director Andrew Strange
Art Director Lynn Jones
Account Director Charlotte Tapp
Creative Director Ben Barrett
Managing Director Claire Oldfield
CEO Martin MacConnol

'wardour'

4 Show them you care
Being proactive about safety and well-being can boost a company's profitability

6 Combined expertise
Chubb employees share their perspectives on the impact of the integration

8 Quiet on set
Time is money in the entertainment industry, so how can interruptions to filming be minimised?

12 Putting a face to a name
The biometric security market should double by 2021, but certain risks are growing with it

16 Target acquired
How to bridge the gap in buyer and seller expectations during mergers and acquisitions

19 From the top down
Employees lodge the most claims against directors and officers, but data protection is among the new risks facing company executives

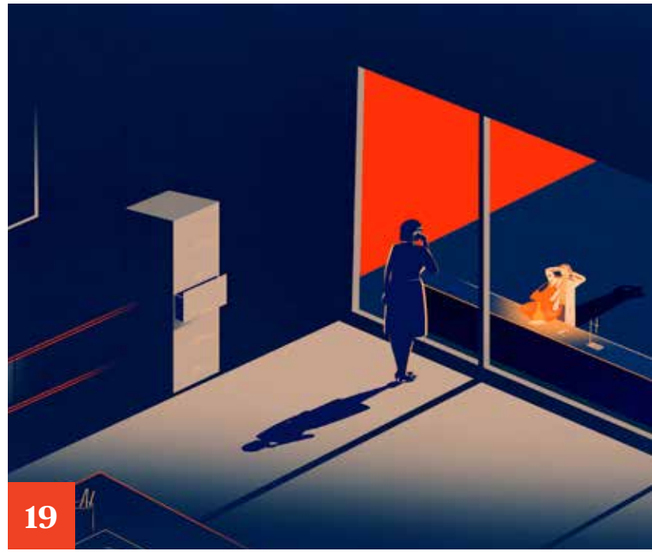
22 Positioning risk managers
FERMA president Jo Willaert says risk managers should be close to decision-makers

24 Troubled waters
How far can you be prepared for unexpected environmental events?

26 Security share
Businesses will soon be affected by the network and information systems directive that European Union member states are preparing to implement

30 Travel safe
With jewellery worth thousands, what should wealthy travellers bear in mind as they pack their prized possessions for their holidays?

16



19

26

Show them you care

Stéphane Baj, Chubb's regional director of corporate and affinity for A&H in Europe, says businesses benefit from ensuring the safety and well-being of their employees

63%
of European companies fully understand their legal DoC responsibilities

54%
provide their staff with flexible working conditions

Duty of care (DoC) is the legal and moral responsibility that employers have to ensure the health, safety and well-being of their employees in the workplace and while travelling for business. Applying it to the highest possible standard is also good for business, according to the latest research by Chubb.

Our report *Reworking Duty of Care* draws on a survey of 240 managers with responsibility for employee duty of care and business travel across the EU. It reveals a correlation between companies that go beyond the minimum DoC requirement and increased profitability, productivity and the ability to attract and retain top talent.

In contrast, companies that fail in providing a consistent level of good-quality care run the risk of exposing their employees to harm, being subject to reputational and financial loss, or underperforming compared with their peers.

The DoC requirement for companies is changing with the times. As the workplace becomes more complex and employees aim to strike a more favourable work-life balance, companies need to ensure that they are proactive rather than reactive in mitigating employee-related risk. That means creating a more pleasant workplace and providing support to employees at all levels of the organisation. As a way to create positive outcomes in an uncertain business environment, duty of care needs to become part of the fabric of the organisation.

While our study shows that almost two thirds (63%) of European companies have a good understanding of their DoC legal responsibilities, there is considerable sector variance.

Companies operating in the oil and gas, chemicals, construction and infrastructure industries are exposed to bigger occupational hazards. They have invested time, money and expertise in hiring specialists to put policies in place. That means they are usually ahead of the game in terms of risk appreciation and deploying best-practice policies that other industries can learn from.

At the other end of the spectrum, some IT, technology and manufacturing companies do not yet appear to adopt best practice. Many companies in the retail and education sectors are also only meeting minimum DoC requirements.

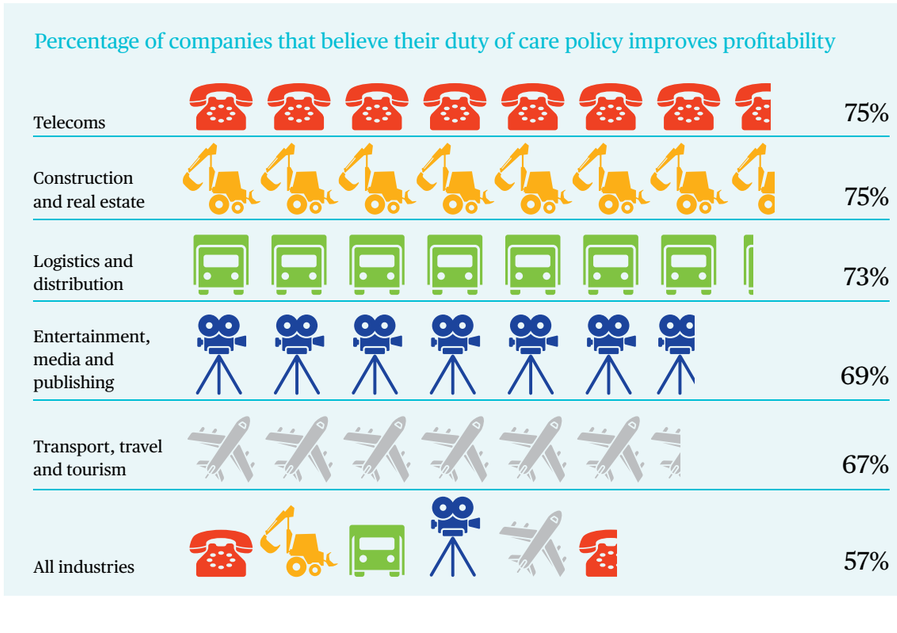
More than half (54%) of respondents said they provided all staff with flexible working conditions for work-life events, but our research finds that smaller companies are more likely than larger ones to offer their employees flexibility: 63% of firms with an annual turnover of US$500 million (€473 million) or less say they offer their staff this flexibility, compared with only 42% of companies with a turnover above US$500 million.

Geographical variations

There are also many well-known cases of leading European companies that produce wonderful social and risk management reports supporting their business activities, but employ workers in very poor and very dangerous conditions in developing countries. When there are fatal accidents, they fail in their DoC and the resulting media coverage can be intense and have a severe impact on their brands.

The 2013 collapse of the Rana Plaza garment factory in Dhaka, Bangladesh is an important case - especially for companies working with third-party suppliers in other countries. The world's media was gripped by the disaster that resulted in 1,129 workers losing their lives, and which led to a compensation campaign organised by workers' rights groups. Many European fashion retailers were identified as failing in their supply chain workplace duty of care.

Our survey shows that a number of companies are subjecting themselves to unnecessary risks because they are failing to insure all of their staff and provide services such as preventive information, post-accident



counselling, or travel-related risk assessments and dedicated travel apps.

European companies can improve many aspects of their DoC offering by seeking more advice from their insurance partners about solutions, tools, apps and policies that help in the smooth and effective running of their businesses. At present, however, just over one in five (22%) of companies seek advice from the insurance industry when they define or update their DoC offering.

Many companies are unfamiliar with the additional support and tools that the insurance industry has developed, such as preventive information, post-accident support, smartphone apps and guidance notes for staff travelling internationally for business. Our research shows that only 34% of companies offer these to all staff, while 23% do not offer them at all.

International travel

Given the proliferation of smartphones and mobile devices, there is great potential for growth in digital services that can support employees, in particular when they travel for business. These tools should be considered a standard offering for all companies that send their staff on business trips. Our research shows that 44% of companies offer a dedicated smartphone app for their staff travelling on international business.

In recent years, we have seen corporate buyers embracing a more holistic approach to managing business travel risks. As a result, we have seen a strong trend away from pure medical expenses and assistance to more sophisticated coverage that embraces these wider risks.

However, our research indicates that understanding of corporate travel risks varies considerably across the region and different industries. This shows that there is significant scope for companies to review their provision and the services that come packaged with it.

We are seeing increased demand for policies with seamless integration of business travel and local group personal accident cover for domestic travel. A good insurance programme can cover these effectively.

As with other sectors within the travel insurance industry, cost containment is an issue for business travel insurers. It is worth making the distinction between cost containment aimed at prevention versus the more blunt approach of tightening policy wording. While we cannot ignore the importance of tightening policy wording if the need arises, we are focused primarily on how we provide the same high level of service and satisfaction at a reduced cost and prevent incidents from happening in the first place.

Tech-powered innovation

Chubb has introduced a number of innovations in the past couple of years in response to the increasing DoC demands and regulation placed on businesses in countries with a high cost of treatment for foreign travellers and expats, such as the US, Hong Kong and Brazil. These are focused primarily on prevention and quick access to our network of assistance providers.

Technology is powering these innovations. Apps and traveller tracking are enabling companies to assist employees on the ground, providing access to medical and security assistance at the touch of a button and real-time alerts highlighting natural disasters and other emergencies to avoid, such as civil unrest or terrorism.

Chubb's Travel Smart technology solution also provides online pre-travel training and certification. It ensures business travellers are fully prepared and made aware of the potential risks and how to avoid them. ■

Combined expertise

Key figures from across Europe and MENA explain how the integration has created an insurance leader with a diverse offering

A bigger array of options

"Our clients benefit now from a broader network and resources to serve their multinational programmes, as well as a larger pallet of products and a client-centric approach with industry-specific products for life sciences, info tech and others."

Ana Coutinho Thomas
Global services manager for continental Europe

Belief in the company

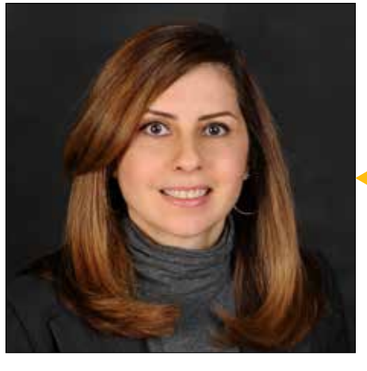
"The strength of our relationships supports the client across the sales, underwriting and claims aspect of the complete Chubb experience. We believe in ourselves. We believe in our name, our brand, our experience, our product and our service capabilities. We believe that we understand what is required and we can deliver."

Diane Davidson
Head of eBroking for UK and Ireland

Embracing change

"The London-based team that I work in is a mix of individuals. We're embracing our differences, observing and learning from each other. And we challenge each other."

Mary McGovern
Management liability manager, London global accounts



Financial strength

"Two great companies, each highly respected in its own right, have been combined to create a global leader in insurance and reinsurance. We are now even better positioned to serve clients by using its combined expertise. Our substantial financial strength provides ease of mind and security to clients."

Mojgan Khoshabi
Regional MD and regional manager, oil and energy for MENA

A commitment to service

"In combination, we bring together a shared belief that claims is at the heart of the business and a great depth of claims talent and expertise. We also bring an absolute commitment to service, building upon Chubb's prior reputation, and a claims culture focused on claims resolution."

Peter Murray
Director of claims, Europe

An enhanced middle market offering

"Middle market and SME clients get access to a broader range of products. Furthermore, international middle market companies can also get the benefits of our global programme knowledge."

Peter Graswinckel
Global accounts segment leader for continental Europe, and global client executive for Benelux

Access to more products

"Combining the two companies was transformational in Benelux. Chubb has strong propositions for companies of any size. From e-commerce solutions for small companies to complex multinational programmes for global companies. Clients now also have access to more products and combined expertise."

Ron Verhulsdonck
Country president for Benelux

Innovative and client focused

"We all bring our own strengths to the table. ACE has always had expertise in multinational programmes and product innovation, while Chubb has had a reputation for quality of service and being close to brokers and clients. Now we have the best of both worlds, setting us apart from our competitors."

Véronique Brionne
Country president for Spain and Portugal

More adaptable

"We have all learnt how to adapt to change. This is an invaluable skill. We are now better equipped to innovate and face the challenges of the future head on. With this new mindset, we will become even more adept at responding to our clients' evolving needs."

Orazio Rossi
Country president for Italy

Quiet on set

Andrew Pring finds out what happens when unforeseen events halt filming, and asks how risks can be mitigated

When Harrison Ford broke his leg on a Pinewood Studios set two and a half years ago, the production schedule for *Star Wars: The Force Awakens* was thrown off course like the Millennium Falcon in a meteor storm.

Losing nearly three weeks of shooting time was a real blow for the film's director and producers, not to mention its injured star. Production costs, already expected to be $200m, would inevitably rise as shooting schedules were redrawn and hire periods for the actors and production crew extended. In a fast-moving business, where time is very big money, delays spell trouble.

But while incidents such as this are clearly serious setbacks, they rarely spell financial disaster in the modern movie business. No major film gets made these days without a production insurance policy in place, and when trouble hits, filmmakers call on the expertise of insurance companies to mitigate the costs of getting the show back on track.

Disaster movie

Every financial backer of a movie project imposes on its producers a contractual requirement to insure themselves against the risk of incurring additional costs. It is not surprising when you consider the host of setbacks that can occur on any film, from injured actors and damaged equipment, through to family bereavements and the calamitous wash-outs that Mother Nature can unleash.

Even common cold sores can be cause for concern for directors, although this is rarely mentioned by the Hollywood PR machine. The close-ups for romantic kissing scenes must be deferred or reshot if an actor is unlucky enough to be indisposed in this way. A bad outbreak of acne or an unpleasant allergic reaction can also cause problems, as was the case when one famous actor was required to don a prosthetic beard.

Emma Vorster, senior film underwriter for UK and Ireland at Chubb, has encountered all these events, and many more, in her time dealing with the world of cinema. "Medical issues are just one of the things we take into account when we're considering cover. We'll look at actors' medical records to see if there have been health issues in the past, and if so, how well controlled a pre-existing condition is and how quickly they recover.

"We also check to see if actors are keen skiers or horse-riders, or pilot their own planes or helicopters. If they are, we ask them to forgo risky activities during filming. We're also wary of actors who like to do their own stunts."

Policies do not just cover the leading actors; key members of the production team working ▶

behind the cameras are also crucial due to the creative input they have.

Equally vital from the producers' point of view is full cover for the expensive kit that is required to make a film. Sophisticated cameras and sound equipment are all vulnerable to damage, especially in unusual filming environments. If damage to kit takes place on a documentary shoot in the Kalahari Desert, filming can be delayed for days while replacement gear is flown in. Emma recalls one cameraman filming on location in Botswana whose camera was irreparably damaged when a monkey dropped on to it from a tree above. It was hard to see the funny side while sitting around for days until a new camera turned up.

Policies for filmmakers are all one-offs, tailored specifically for each individual project. Daily filming costs are examined in great detail by insurers to see where the money is being spent and establish where the main risks might be before cover can be costed. Risks can alter considerably from one film to the next – costume dramas and sci-fi, for example, present different challenges.

TV series, which are often in constant production mode, need a different type of cover. "We can provide annual policies for these film companies, and this gives them the freedom to get on with their business," says Emma.

Cover enhancements

As well as protecting against business interruption, third-party property damage and illness or injury to cast and crew, insurers are always developing new ways to adapt to the needs of filmmakers. One innovation that has proved useful is a civil authority clause to cover cancelled events or street closures that lead to filming delays. When New York's world-famous marathon was cancelled as Hurricane Sandy tore its way up the Eastern Seaboard in 2012, the TV producer covering the race was able to reclaim its costs thanks to this extension. Other recent enhancements to insurance policies cover new camera technology, wider age limits, utility supply failure and mechanical breakdown.

Claims are actually quite infrequent: filmmakers are highly professional and used to protecting their human and physical assets. But when they do happen, they can be for serious amounts – sometimes millions of dollars and quite often hundreds of thousands.

When accidents do happen, claims handlers work closely with the filmmakers to discuss the best way to reschedule production. "We can either handle the claim in-house or, if there are complications, we work with some very good loss-adjusters who meet with the film producers and discuss the best ways to redress the situation," says Chubb claims examiner Rachel Fitzgerald.

After a lead actress broke her ankle on a major film recently, doctors said she would be off for two months. The film required her to do a lot of running, so to help her get back on set as quickly as possible, the insurance team installed a special padded running track that would absorb any pain she felt. They also employed a physiotherapist to accelerate her recovery. When she was well enough to run on the track, some scenes were reshot with the director focusing the camera purely on her upper body.

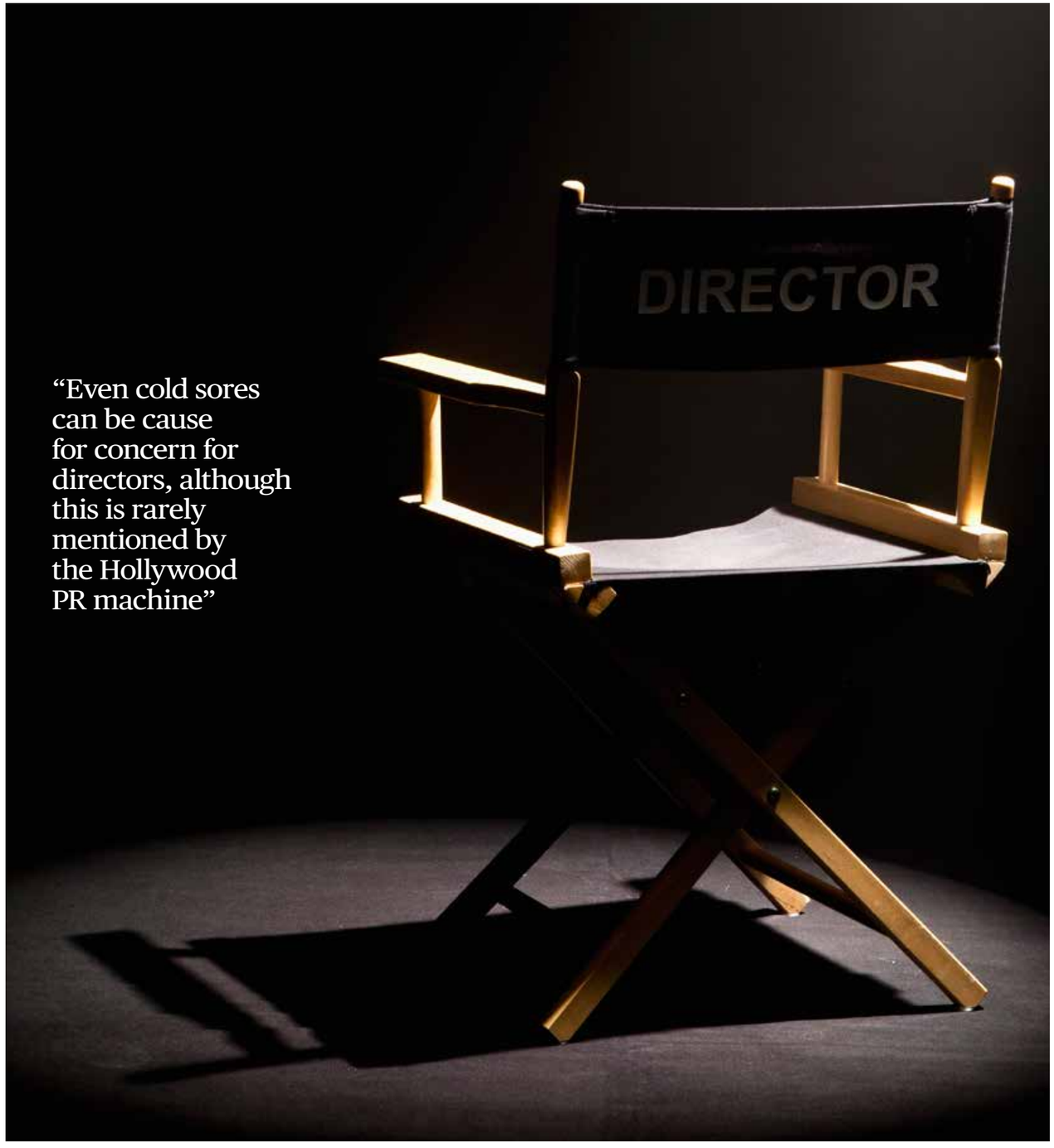
Similarly, when the actor mentioned earlier had an allergic reaction to a prosthetic beard, a dermatologist was brought in to alleviate the skin condition and the actor was back on set in no time.

Grey areas

Not everything that goes wrong during filming is claimable. "Some events are predictable and may therefore not be covered. For example, in a desert, did the client take steps to protect against dust ingress, and were the cameras suitable? But in grey areas, we try to favour the insured and not decline. We don't have many exclusions and we aim to be as fair as we can," says Rachel.

Grey areas are not uncommon in this industry, where the weird and wonderful are commonplace. Rhona Alsworth, a film production specialist at insurance brokers Integro Entertainment, recalls a film in which the director wanted to build an aluminium house that was to be floated into the air by balloons using a new technique. "We talked to Chubb about how it could be covered and they came up with a way to do it. We like people who are good at thinking outside the box."

We are always told there is no business like show business, but it is clear that the show could not go on without the insurance business backing it. ■



"Even cold sores can be cause for concern for directors, although this is rarely mentioned by the Hollywood PR machine"

Top tips for risk managers

Never forget financial exposure
Producers, directors and their associates operate at intense levels of physical and mental stress. With so much going on during filming, they can overlook or forget their contractual obligations when it comes to risk avoidance. But if they are not mindful of their financial exposure, knock-on costs can snowball out of control.

Seek a tailored insurance policy
The production of every film is different. That means there is no one-size-fits-all policy to cover any eventuality. It is crucial that filmmakers help insurers tailor the policy to the unique needs of each individual production.

Avoid delays by assessing risks early
Timing always goes down to the wire in filmmaking and things move very fast. Yet insurance is often well down producers' list of priorities. By factoring it in earlier in the schedule, last-minute hold-ups over cover can be avoided.

Get in touch

If you would like to discuss any of the issues raised in this article, please contact Emma Vorster at evorster@chubb.com

Photography: Getty

Putting a face to a name

Biometric security offers new convenience for users, but what risks are companies taking when they roll out this technology? **Paul Rubens** finds out

Imagine a world where you can walk up to a cash machine and withdraw money without using a card or entering a PIN. Or a world where you can order groceries online without even entering a username and password. That is the promise of biometric authentication. In contrast to password verification, which relies on you providing something you know, biometric authentication relies on something you are: a fingerprint, a sample of your voice or, in the case of facial recognition, a clear view of your face.

The benefits of biometric authentication are obvious - you can forget your password or lose your card, but you cannot forget or mislay your fingerprint, your voice, your face, or any other physical feature. Convenience is also a factor, as looking briefly into a camera, for example, is much easier than typing in a long password.

For these reasons, biometric products are increasingly popular: research firm MarketsandMarkets forecasts that the global facial recognition market alone will grow from around US$3.3 billion (€3.1 billion) in 2016 to US$6.8 billion (€6.5 billion) by 2021. Biometric technology is likely to be deployed in almost every sector of the economy, from facial recognition in hospitals, to fingerprint scanning on construction sites, to voice recognition on telephone banking services.

Determined hackers

But biometric security is not impregnable. Many biometric readers, especially more affordable ones, such as those found on smartphones, digitise some of the biometric information. This data is put through a cryptographic process called 'hashing'. The biometric data captured is equivalent to a medium-length password, which means that a determined hacker could get around the safeguard in many cases, according to Karsten Nohl, a member of German security collective Security Research Labs.

"A complex password is virtually uncrackable, and a fingerprint can't be better than that," he says. "It may be better than a simple password, but not better than a strong one." And hacking some voice recognition systems is trivial: "You can pretty much make any voice sound like any other." Karsten has also demonstrated that an iPhone fingerprint reader can be fooled using an imitation finger sprayed with graphite to simulate the properties of skin.

However, there are a number of ways to enhance the security of biometric authentication systems. One technique is to combine several different types of biometrics and other information, such as the location of the user and the time of day, at the same time to build a complex profile of that person. This creates a digital portrait that can be used to recognise them, and which is harder to forge. ▶

"Biometric technology is likely to be deployed in almost every sector of the economy, from hospitals, to construction sites"

Assuming that the biometric system is well designed and cannot easily be fooled by someone with an imitation finger or photograph, the biggest risk is that a hacker somehow gets hold of the biometric data stored by a company - the equivalent to someone making off with a list of passwords.

The oft-cited problem with biometric data is that while customers can change their passwords, they cannot change their fingerprints, their voice or their face. In theory that is not a problem because a company can 'salt' digitised biometric information by combining it with a random piece of data before hashing it. That way, if the information is compromised, new biometric data can be generated by re-enrolling users and combining the newly captured biometric data with a different salt, which is the biometric equivalent of changing every user's password.

Yet many companies do not carry out hashing, says Karsten. When it comes to fingerprints, some actually store the fingerprint information in a form that is close to the original, with no hashing - perhaps so that users can log on using different fingerprint readers. "Some systems store the exact image that the reader captures when it reads a finger," he says. "So all the information you need (as a hacker) is right there."

New data, new risks

This has important implications if customers' biometric data is stolen, according to Matthew Clark, director of global markets at insurance broker La Playa. "Biometric data is a measurement of physical traits, so it could be seen as something akin to medical records data," he points out. "That means there are serious data-related exposures: if you allow a data breach through negligence, that could land you in hot water with regulators," he says. "Even if the breach is due to third-party negligence you could face the costs of a regulatory investigation, notifying customers, and many others."

When it comes to regulations, Matthew stresses that anything relevant to personally identifiable information is likely to apply. Biometric technology is also likely to fall directly within the scope of new regulations. "Regulators are evolving the law in this area, and people drafting new laws are aiming to make them as futureproof as possible," says Matthew. "So, for example, biometric technology will fall within the scope of the EU's General Data Protection Regulation." This comes into force in 2018, replacing the 1995 Data Protection Directive.

The impact of this regulation could be significant, warns Karen Strong, technology manager for UK and Ireland at Chubb. "The new EU data regulations will introduce penalties (as well as new procedures and appointments) for an insured where they are in breach of security with regards to third-party data. The regulations will impose strict controls over personal data and the fines for not adhering to these are significant," she says.

Fines and penalties are only covered by insurers where they are legally insurable and the insured is legally liable. "In the UK, though, legal fines are generally not insurable, although cyber insurance forms will provide cover for regulatory fines (other than those uninsurable, such as criminal fines) following a data breach," says Karen.

More generally, she advises that if biometric data is held in a form that can be defined as personally identifiable information, it gives rise to privacy risk. "With Biometric data, breach of privacy is probably the biggest risk for a company hosting this data, along with the subsequent first-party consequential losses associated with a breach," explains Karen. Insurers take this into consideration when assessing risk. "Points we would discuss with an insured, bearing in mind all of our clients are providers of technology, could include what steps need to be taken to ensure that the personal data they host is not used for any other purpose than that agreed to by the individual," she says. "Therefore, we would consider how they keep the data safe; is it encrypted, separated and stored in multiple places; what is their systems security like; and are they ISO 27001 accredited or PCI compliant?"

Understanding the supply chain is also important for providers of technology and insurers alike. "We would work with a client to assess what risk any of their service providers represent: what quality controls do they have in place, both physically and contractually, and what security measures do they have in place to secure the data," says Karen.

Another factor taken into consideration is the risk of underlying technology failing. Karen says: "We would be assessing the quality assurance procedures of the technology provider - are they documented and fully effective, how has the software been tested prior to launch?"

There are also risks beyond the more obvious crime and security breaches. For example, Karen asks: "What would the impact be if an age verification system failed to work properly? If alcohol was sold to an underage person because a biometric identification system was flawed, what would happen if they then injured themselves or caused injury to others?" These would be third-party insurance considerations, but it is also important to consider the potentially significant first-party costs associated with 'reworking' the biometric data following a breach.

Breach of privacy

"As insurers, we have to consider our clients' exposures from both a first- and third-party perspective. There are immediate first-party expense risks for those responsible for data and the associated notifications in the event of a breach, along with legal liability exposure in respect of pass-through fines and penalties presented as damages awarded for the failure to deliver a secure service and protect the personal details held as biometric data," says Karen.

While it is still early days for biometric authentication, Karen firmly agrees with the MarketsandMarkets research that predicts its influence will increase rapidly. "My personal view is that without a doubt this technology will grow in significance in our every day lives, and subsequently the insurance market needs to be prepared to respond, from both a risk assessment and cover perspective," she concludes. ■

€3.1bn
The value of the facial recognition market in 2016

€6.5bn
The projected value of the facial recognition market in 2021

Top three tips for risk managers

1. Biometric data should be altered ('salted') and run through a cryptographic process ('hashed') before it is stored. If this is not done correctly, data is likely to fall into the category of personally identifiable information, and a security breach could have serious privacy implications.

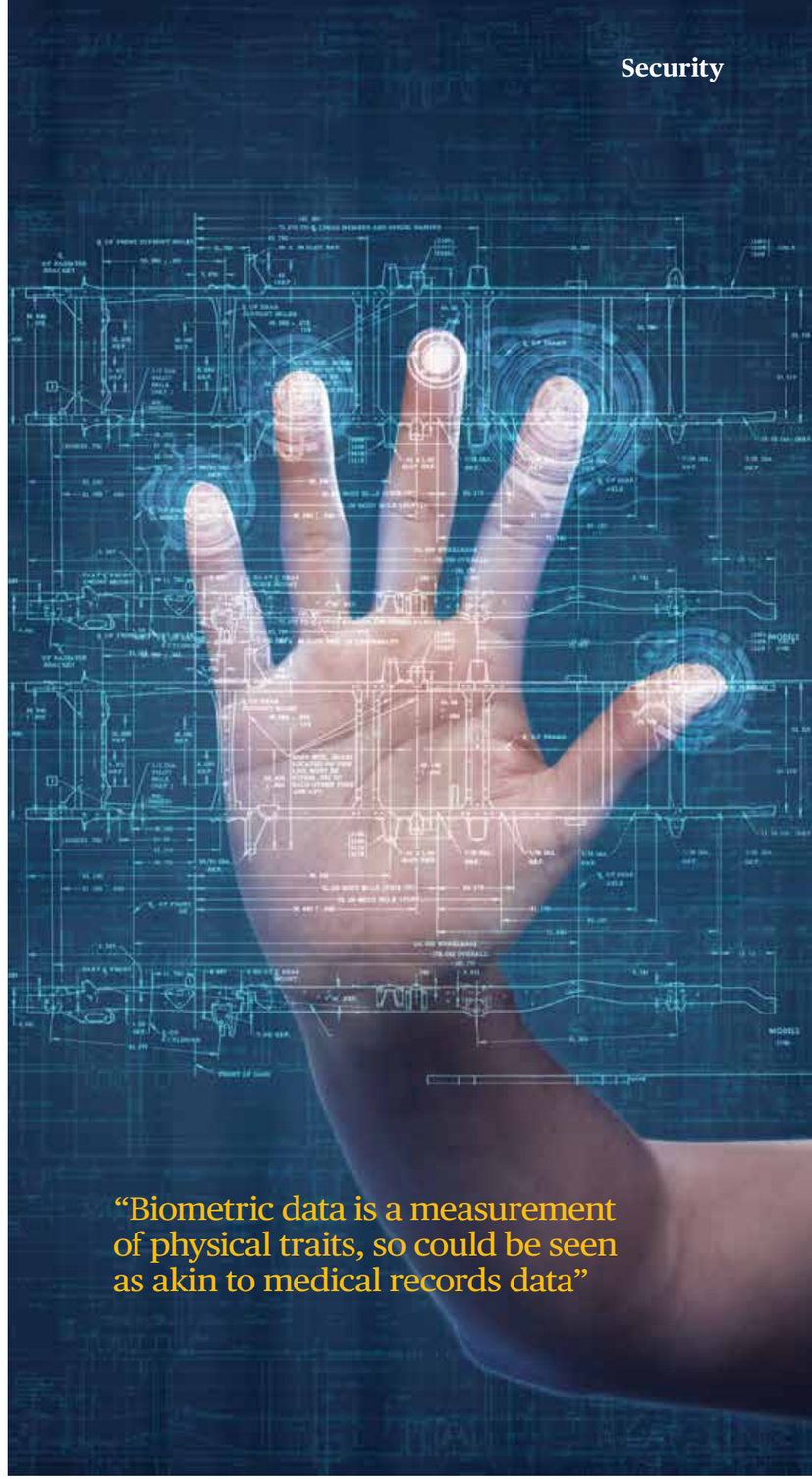
2. This technology will fall within the scope of the EU's new General Data Protection Regulation, which comes into force in 2018.

3. Security breaches are always expensive, but if users of biometric authentication systems have to re-enrol themselves (for example by supplying fingerprint information) then this can be more expensive and time consuming than asking users to change their password.

Get in touch

If you would like to discuss any of the issues raised in this article, please contact Karen Strong at kstrong@chubb.com

Photography: Getty



Target acquired

Merger and acquisition (M&A) transactions can falter for a whole host of reasons, but there are ways of bridging the gap between buyers' and sellers' expectations, says **Stuart Collins**

The volume and value of global mergers and acquisitions dropped in the first half of 2016, following a record year in 2015, according to the Zephyr M&A database. Nevertheless, there were still some 43,352 deals worth a combined US$1.94 trillion (€1.8 trillion) in the opening six months of the year.

The reasons behind M&A trends lie largely in macroeconomic factors, but on a micro scale, deals can unravel when the main parties do not see eye to eye over how to deal with ongoing liabilities. Long after the champagne corks have popped and the transaction is complete, substantial liabilities continue for both buyers and sellers. Unsurprisingly, buyers seek assurances that they are not acquiring costly future losses and due diligence may uncover, for example, potential liabilities associated with tax arrangements, past M&A activity or cyber risks. ▸

From the top down

Being a company director or officer involves risks well beyond mere compliance with criminal law. **Andrew Cave** explores how those risks are evolving

When the dotcom bubble burst, a slew of director negligence, fraud and breach of fiduciary duty lawsuits followed. The global financial crisis of 2008 then had an even greater effect in spurring legal action against directors and officers (D&O). But what will be the top threats they face in coming years, and how can they be mitigated?

"Shareholder class actions account for the largest D&O cases and often result in huge settlements," says Michael Lea, senior vice president for global professional and financial risks at insurance broker Lockton. Even cases that are dismissed can cost a company up to US$5 million to defend.

"The incidence of securities class actions is at its highest since the financial crisis and the risk of investigation by the US Securities and Exchange Commission (SEC) for violation of securities laws is also significant," adds Michael.

However, the highest number of claims comes from employees, including employment practice violation allegations, injuries, fatalities and fraud claims. Responsibility flows up to directors ▶

"Tax liabilities, cyber exposures and Brexit are some of the issues concerning buyers today"

"In today's uncertain environment, buyers are likely to be more cautious when committing money and may be more likely to walk away if they are not comfortable with the risks or their ability to recover potential losses under warranties and indemnities," says Richard Britain, international head of transactional risk at Chubb.

Over the years, transactional insurance has proven to be a facilitator of M&A deals. The product first gained popularity among private equity companies looking to limit their liabilities under warranties and indemnities, but recent years have seen an increase in corporates buying transactional insurance, as awareness of the product has increased and as M&A lawyers have become more comfortable with it. Tellingly, London-based insurance broker Marsh saw take-up of transactional insurance continue in 2016, even as the number of M&A deals dropped. In the first half of the year, it reported a 35% increase in limit in Europe, the Middle East and Africa.

Transaction insurance is no longer just used to get a clean exit for private equity, says Christopher Jackson, senior vice president and head of UK transactional risk at Marsh. Around 44% of policies are now purchased by a corporate as companies use transactional risk insurance to better compete for assets, especially in auction situations, he says.

It is now being used to facilitate deals on a wide range of private M&A targets, from special-purpose vehicles holding assets, such as real estate and renewable energy assets, to technology, leisure and manufacturing companies, according to Richard.

"While it is not a replacement for good due diligence, insurance can help overcome genuine issues or a mismatch between the buyer's and seller's positions," says Richard. "It is all about finding solutions to help deals proceed where they otherwise might not."

According to Christopher, there are three ways in which transactional cover can oil the wheels of M&A transactions: by resolving differences on contractual terms; by addressing concerns over recoverability; and by facilitating acquisitions in new jurisdictions.

When differences emerge between the buyer's and seller's expectations on future liabilities, warranty and indemnity (W&I) insurance can be particularly useful. For example, a buyer may have concerns about liabilities that come to light during due diligence, but the seller is unwilling or unable to provide adequate warranties and indemnities. "Transactional insurance can limit the seller's ongoing exposure while at the same time giving adequate comfort to buyers," says Richard.

Gaining confidence overseas

Cross-border deals, particularly in unfamiliar markets, can also present political, legal and credit risks for buyers. Investors may have concerns around recoverability under the warranties and indemnities provided by sellers. For example, the financial strength of the seller may be more difficult to gauge in a foreign market, and the outcome of disputes heard in local courts can be difficult to predict. Transactional insurance can give buyers more confidence when making acquisitions in new markets, explains Christopher.

M&A deals also run aground when specific liabilities emerge during due diligence. Tax liabilities, cyber exposures and Brexit are some of the issues concerning buyers today, although other liabilities could include past M&As, ongoing litigation, environmental, intellectual property and employment liabilities.

Transactional insurance can ease buyers' concerns over these specific liabilities, explains Richard. "Where a buyer has a concern, such as with a potential tax liability, the underwriter can take a view and price the likelihood of the risk arising," he says.

Although in some cases certain risks will be excluded from a W&I policy, such as environmental or cyber risks, it is possible to develop tailored solutions, explains Richard: "We can work with our environmental liability colleagues at Chubb to create a solution that combines W&I insurance with environmental cover." Cyber, environmental and product liability are all 'known risks' where buyers may have concerns, and where insurance can be of assistance.

This approach can also help transactions where there are uncertainties around land title and planning, as is sometimes the case with renewable energy projects. Title insurance, which can be used standalone or in tandem with W&I insurance, can give lenders the confidence to release capital ahead of gaining planning consent, enabling a deal to go ahead, explains Christopher.

Stuttering economic growth in some markets and the UK's vote to leave the EU may mean a further slowing of M&A activity in the short term. "Deals are taking longer to get over the line and buyers are more cautious on due diligence. But this is where transactional risk insurance can come to the fore and we believe its value to clients will only rise," says Richard. ■

Photography: Sara Morris; styling / art direction: Sandy Suffield

for failure to supervise or impose adequate controls and procedures. An increase in whistleblower bounties, offered by the SEC and other regulators, has also led to a higher incidence of claims initiated by tip-offs. Lawsuits against company directors tend to follow investigations or enforcement actions by government agencies, such as the US Department of Justice and the FBI, or regulatory bodies, such as America's Food and Drugs Administration.

US deputy attorney general Sally Q Yates stated in a 2015 memo: "Civil attorneys investigating corporate wrongdoing should maintain a focus on the responsible individuals, recognising that holding them to account is an important part of protecting the public."

In the UK, the Companies Act of 2006 stipulates more than 200 offences that may result in action against an individual director or officer. Michael says the cost of defending such actions has increased significantly as senior officers now require separate legal counsel to address the different duties imposed on them under the Act. These duties are addressed in eight sections of the Act and are much more comprehensive and codified than they were previously.

A new data protection regime

The General Data Protection Regulation comes into force in the European Union in 2018, strengthening individuals' rights over information held about them. Non-compliance could result in fines equating to 4% of global turnover and company directors may be held responsible for reporting breaches.

Luis Aguilar, the Democratic commissioner of the SEC from 2008-15, made it clear while in office that the safety and security of customers' personal data is the responsibility of every director of every board of a public company. "Data protection has never been higher on the agenda for companies of all sizes in all industries," says Steve Bear, Chubb's London corporate management liability manager for financial lines.

Steve believes the adoption of the new EU data protection framework poses as many risks to individual directors and officers as it does to the companies they run. "The duty of data protection officers should not be overlooked or confused with that of compliance officers," he says. "There are heightened expectations for data protection officers, who need to have an in-depth understanding of the company's procedures surrounding the management of personal data. Failure to adopt and implement adequate safeguards stipulated by regulators can lead to costly investigations and legal actions.

"Data protection officers have to answer to the regulator itself rather than the board of directors. Several high-profile cases have seen traditional cyber breaches result in D&O claims, with officers called to account for the quality of the insured's IT security infrastructure," adds Steve.

The third wave of cyber crime

According to Bogdan Botezatu, senior electronic threats analyst at internet security group Bitdefender, we have now entered the third wave in the history of cyber crime.

The first was the preserve of bored teenagers and jobless graduates in Bulgaria, Russia and other Eastern European countries with a high standard of technical education. It was more about anarchy and freedom of expression than making money. But the second wave saw organised mobsters send phishing and other scam emails by the millions in the hope of duping a tiny percentage of individuals into parting with cash.

The third wave involves the deployment of ransomware. This technology encrypts photographs and other personal data on an individual's computer or on a company system, informing victims that the material will be lost in perpetuity unless an untraceable payment is made in Bitcoins.

"At the moment, there is little way of combatting the ransomware once it has got onto a system or computer," says Bogdan. "This is going to pose a lot of problems for businesses."

Riskier human resources

Another risk is the employment of illegal workers, which will attract tougher penalties under the UK's Immigration Act 2016. This increases the maximum custodial sentence for company directors and owners on indictment from two years to five. Mitigation includes being able to prove that an employer has conducted appropriate checks.

Environmental liability should also be on the radars of directors and officers. Taking companies and their directors to court over water contamination, waste and air pollution, damage to rainforests and other natural resources infringements is now a major weapon for environmental campaigners. Companies are advised to have environmental policies and standards in place and to be able to demonstrate good records of compliance with regulations and voluntary testing.

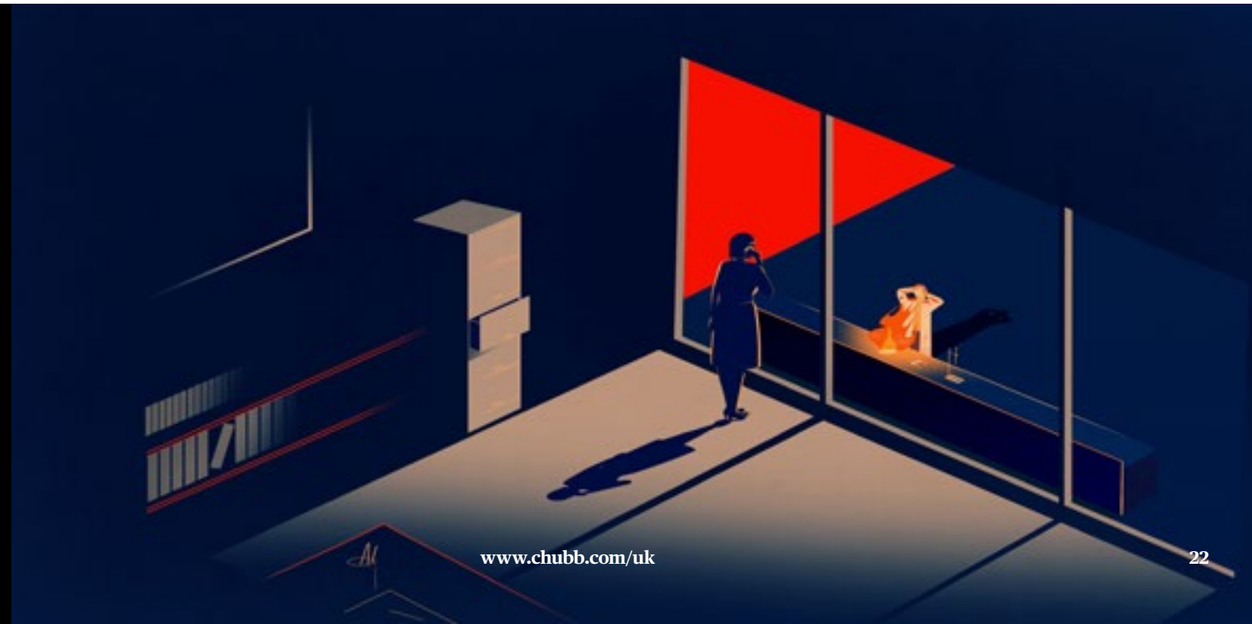
With new risks emerging all the time, it is important that directors and officers stay informed about their responsibilities and have adequate insurance cover in place. ■

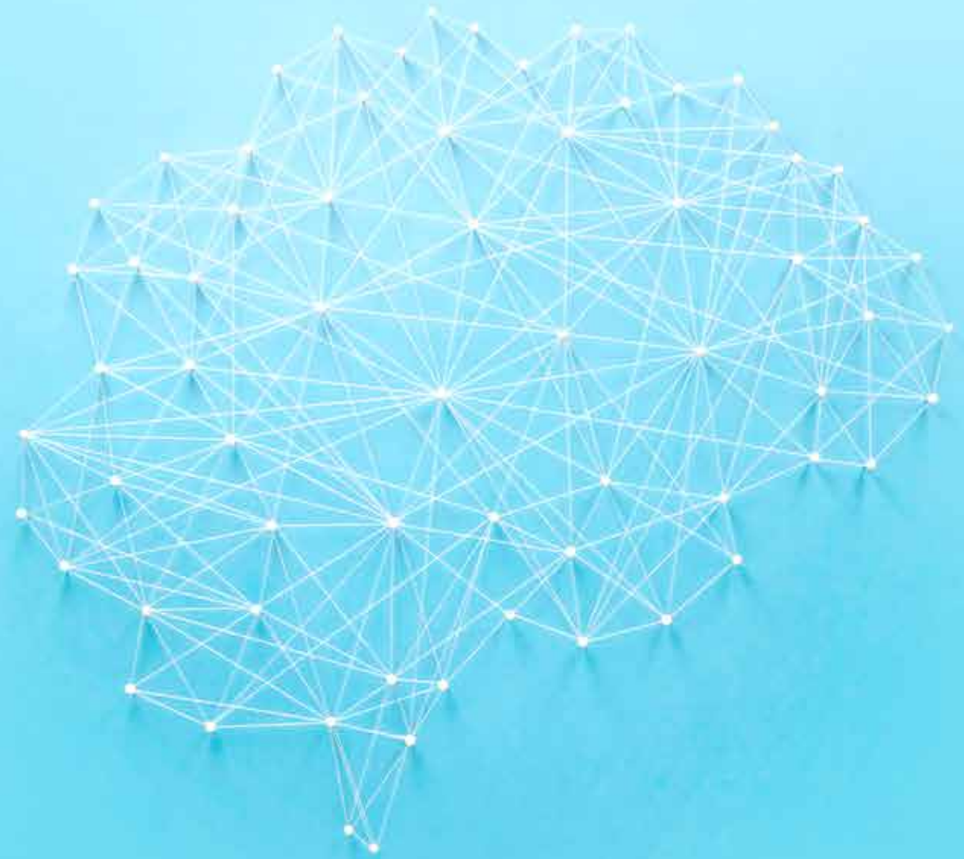
"Environmental liability should also be on the radars of directors and officers"

Five tips for risk managers

- Demonstrate awareness of new and existing laws, document procedures and policies and keep on top of regulatory changes, new social habits and emerging risks.
- Show that your company goes beyond legal requirements to protect against data, cyber, financial markets, social media, employment and environmental risks.
- Ensure that designated individuals are in charge of major risk areas, such as data protection, employment relations and environmental impact, but also make it the job of everyone in the company to monitor and report risks.
- Do not try to do it all yourself. Get reliable professional advice on risk management and its mitigation.
- Be alert to constantly changing risks. Tomorrow's risks will not mirror today's exactly.

Illustrations: Matt Murphy





Positioning risk managers

FERMA president **Jo Willaert** tells *Progress* why risk managers should play a key role at the heart of any successful organisation

It is perhaps not surprising that the president of FERMA, the Federation of European Risk Management Associations, should be a strong advocate of the importance of risk management for European businesses today. But for Jo Willaert, risk manager at Agfa-Gevaert and current president of FERMA, it is not just risk management, but the role of the risk manager that he is most passionate about.

Jo firmly believes that the risk manager has a leadership role to play when it comes to the company's strategy and business plan. "By leadership, I mean the position in the company to support the decision-making process of the company – the risk manager supporting the overall strategy," he says. "Leadership means that the risk manager should know what the targets and strategy of the company are, in order to support the company and to make sure the risks that could be an obstacle to reaching these targets can be managed."

So, for Jo, it is important that the risk manager is visible in the company, and close enough to the decision-makers. "The risk manager does not make the decisions, but he or she should be informed about the decision-making process and give advice on it. It will then be up to the decision-makers to do with that advice what they want. Senior management and the board are supported by internal audit, financial and legal functions, and risk management should be on an equal level," he says.

> "It is not enough to say what the risks are. Before you do that, you have to listen, and listen actively"

One of the difficulties for the risk manager is the negative connotations of risk. But according to Jo, risk management delivers a positive message. "The risk manager is not there to be an obstacle, just to give reasons as to why the risks are too high to do the business. The risk manager is there to explain to decision-makers the risks of their business plan. Then they can decide how to proceed knowing what the risks are and how much they can be managed. In this way, risk management should influence the strategy and business plans."

Once the strategy is decided, he explains, the risk manager can come back with a plan for managing the risks in such a way as to make a success of the strategy. "It is a positive message and certainly not one that makes people afraid of taking risks. On the contrary, we support risk-taking, because risk-taking is part of entrepreneurship," he says. "We try to manage, help and give methodologies and analyses to make sure that the risks are known and under control."

Leadership was one of Jo's priorities when he became FERMA's president, together with communication and education. Communication, he believes, is a key skillset for the risk manager, but it is one that applies at all levels of the company, whether it is with people in the field or the board.

"It is not enough to communicate; you have to do something with that communication," he explains. "It is not enough to say what the risks are. Before you do that, you have to listen, and listen actively. By that I mean listen to what the decision-makers are saying, listen to what the people in the field are saying and listen to what the customer and suppliers are saying.

"The risk manager must have access to everyone involved with the risks. But at the same time, risk managers should be strong enough to say what they have to say independently."

The education aspect is where FERMA has been most active so far. FERMA's professional certification programme, rimap®, was launched last year, providing a programme of European Certification for professional risk managers, giving independent confirmation of the professional competences, experience and standards of individual risk managers, and accreditation for the risk management programmes of educational bodies. In October 2016, at the FERMA Seminar in Malta, the first 18 risk managers received their rimap certification.

Recognition

What's next for the profession? For Jo, to be a successful risk manager you need three things. "First, you have to be trained, which is why FERMA is talking about rimap – you need a theoretical basis and you need to know what you are talking about," he says. "Next, you need experience, and that can be in any company, in any situation, but you do need the experience of managing risk. And third, you need to know your own company. If you do not know the culture of your company, you will fail. Your advice will not be taken into account. It is important to adapt your style to the culture of the company."

Increasingly, he says, the role of the risk manager is more difficult because you cannot fit the job of risk management in a box. "Risk managers touch everything. The risk manager is linked with IT, with legal, with internal audit, with all the aspects of the company. So in that sense, the role is now more difficult. But if, at the same time, the decision-makers in the company are increasingly recognising the importance of the risk management function, then it is easier, because of the support they provide. Without doubt, once your job is recognised within your company, and you are there as an equal partner, at that moment your job is easier than it was before," he says.

That is what Jo wants to emphasise more than anything else – what risk managers require now is recognition. The responsibility of risk management is increasingly a strategic one, and he believes that when risk managers are recognised as supporting the decision-making process, then their companies will get full value from the important role they have to play. "Recognition is there for risk management as such, but I think the next step is that it should be centralised in the function of the risk manager. A lot of companies will say that they do risk management; they have a quality manager, human resources, health and safety, and security, and so on. But there is no common link with the strategy of the company, and this is what the risk manager is all about – making sure that the strategy and the business plan of the company will be successful and that targets will be reached. For that you need a recognised individual. There, I think, we still have a way to go." ■

Lessons for risk managers

Take a leadership role
Know the company's targets and strategy in order to manage the risks that present obstacles to those aims.

Send a positive message about risk
Let the company know that risk managers exist to support and inform risk taking rather than obstruct the process.

Listen to everyone involved with risk
From the suppliers and people out in the field to decision-makers, actively seek out the views of everyone involved in a risk, but be strong enough to speak with an independent voice.

Understand company culture
In addition to having the knowledge and experience to be successful, adapt your styles to the culture of the company.

Recognition is vital
Use opportunities to get recognition, including through your risk management associations. The role becomes a lot easier once risk managers are properly recognised within their organisations, particularly by decision-makers.

Photography: Getty

Troubled waters

Pollution incidents can happen when they are least expected. **Marcus Alcock** finds out how companies can be prepared

Despite a much more stringent regulatory focus on environmental pollution in recent years, and the best efforts of risk managers, pollution incidents will continue to dog even the best-intentioned businesses.

Just look at Caterpillar Northern Ireland, which made the headlines in the summer as the source of a big diesel spill off the County Antrim coast. According to the company, the diesel had found its way into a storm drain that runs out to the sea, and was part of a bigger on-site spill.

As Nicky Eury, a principal at environment and health consultancy firm Ramboll Environ, points out, although the majority of companies apply good environmental management practices, human and infrastructure failings are still commonplace.

"Even though there are a lot of responsible companies out there, the fact is that accidents will always happen. And it can be difficult to identify significant bottom-line risks, particularly in the case of acute pollution [sudden and accidental], whereas historic contamination issues are somewhat easier to predict," says Nicky, who has more than 25 years' experience in corporate environmental risk management.

Besides, she adds, the most concerning issues are not necessarily the high-profile incidents that tend to make the press, but what she calls 'mid-point' ones. "For example, a watercourse that is located in a sensitive setting could suffer significant environmental damage, even though the same level of spill in another system may cause little harm."

However, historic site contamination can also come as a surprise. In one incident, a solvent plume was discovered on an adjacent property when the foundations of a new development were sunk. The source of the pollution was identified as printing operations that had taken place on the property 20 years earlier. The original polluter could not be found, so the current owner was held liable for €300,000.

Chubb's Robert Latimer, an underwriter specialising in environmental risks, agrees that there is a wide spectrum of risk. "Here at Chubb, we're used to dealing with a lot of incidents, ranging from small-scale industrial units to multi-million-pound clean-ups resulting from a wide range of industry sectors," he says. "Some clients think that if nothing has happened previously then nothing can go wrong in future, so the real question becomes: what risk management do companies have in place?

"And what happens when something goes wrong? After all, it can be a long and arduous process dealing with an incident, and then there's the media aspect. Being investigated by the regulators and splashed over social media can leave a huge dent in your reputation, and result in significant legal costs."

He recommends that companies ask whether their existing insurance policies cover offers enough protection in the event of a pollution incident. "Environmental impairment liability (EIL) cover has expanded significantly over the years to encompass areas that it perhaps didn't previously, so that it's now cost effective and is tailored to the client. So if we look at some of the recent incidents, standalone EIL cover is fit for purpose to deal with them, unlike some of the more traditional property and liability coverages."

Robert also suggests that companies seek insurers that can offer strong crisis response. "Environmental claims often come with a reputational impact, which companies should ensure is included in their cover," he says. ■

Photography: Getty

EU member states are preparing to implement new rules on cybersecurity that mean certain attacks need to be reported. **Simon Creasy** asks how businesses will be affected

In its 2016 *Internet Security Threat Report*, global cybersecurity consultancy Symantec revealed a scary series of statistics. In 2015, more than 430 million new unique pieces of malware were discovered, up a third on the previous year. The number of detected 'zero-day' vulnerabilities (holes in software unknown to the vendor) more than doubled and 'spear-phishing' campaigns (emails requesting confidential data) targeting employees grew by 55%.

Thanks to numbers such as these, there is a growing acceptance among companies that it is no longer a case of whether hackers will attack, but of when. This acceptance has been accompanied by a strategic shift from attack prevention towards attack detection and rapid reaction to minimise financial and reputational damage to businesses.

But in an increasingly interconnected and borderless digital world, a successful attack on a business in one country can have a knock-on effect on another business elsewhere. This means that if you do not adopt a consistent approach to security across different countries and continents, you are leaving weak links that could be the access point of an attack.

To address this issue, the European Commission approved the EU's first ever cybersecurity rules in July 2016. Member states have two years to implement the directive on security of network and information systems (known as the NIS Directive), which places new requirements on digital service providers and operators working in essential areas such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors will be expected to take appropriate security measures and notify national authorities of any serious incidents.

So what are the main challenges around implementing these new controls?

Easy targets

Despite the security industry making significant improvements to cyber protection software, the scale of the threat to businesses has grown over the past few years. Companies no longer have to contend with just the threat of hacks carried out by criminal gangs or lone-wolf attackers - there is also the growing danger of corporate and economic espionage being carried out by nation-state-sponsored attackers.

And worryingly, it is getting easier for hackers to carry out these attacks, says Roger Francis, senior strategic consultant at cybersecurity firm Mandiant, a FireEye company. "From a capability perspective, the bar is lowering," explains Roger. "There are a lot of tools out there and the ease with which attackers can leverage those tools is increasing the cyber threat posed to businesses."

The slow pace of detection is also concerning. Looking at cases it dealt with in Europe, the Middle East and Africa in 2015, Mandiant found that the average time to discovery of a cyberattack was 469 days.

Transparency is critical to cybersecurity, as is data sharing, but the job of these hackers is

"The scale of the threat to businesses has grown over the past few years"

430m
The number of new pieces of malware discovered in 2015

1/3
The rise in detected malware in 2015 over the previous year

being made easier because there is currently no consistency of approach at a government level across Europe. Therefore there are "no consistent requirements on industry and commerce about what protections they need to put in place", says Nick Bellamy, senior information and network technology specialist, risk engineering services, for UK and Ireland, at Chubb.

This is particularly important when it comes to companies that are responsible for running essential services, as well as digital service providers – hence the long-overdue introduction of the NIS Directive.

Central record of attacks

"The government can only do something if it knows about attacks, and a lot of these essential services are now in the hands of the private sector. That's why the EU is introducing legislation so that companies running essential services will need to report incidents to a central body, in order to work out where the threat is coming from and protect against it," says Hans Allnutt, partner and leader of DAC Beachcroft's cyber risk and breach response team.

The cybersecurity community unanimously agrees that the new directive is a good idea, but some question how it will be implemented. Because it is only a directive, EU member states must decide for themselves how to incorporate the provisions of NIS in their national law, which means we could see what Nick describes as a "patchwork quilt" approach.

"It's a great start – the problem is it's a directive and not a regulation," says Nick. "Therefore all member states have two years to come up with their own version of it, which they can then implement, but that doesn't ensure consistency. It will be different from country to country. So the way the UK approaches NIS and the minimum requirements and standards it introduces will probably be different to, say, Portugal."

There could be further differences around the interpretation – both between companies and countries – of what actually constitutes a breach, says Roger. "The question of when an incident is declared is an interesting one, because within different organisations the definition and spectrum of what constitutes a breach is a bit of a grey area," he explains. "Companies need to be sure that they have a defined escalation matrix, because without one, it will be hard to take appropriate action when they may need to declare a breach."

"With the clock ticking on the implementation of NIS, some member states are in a better position to implement the directive than others"

With the clock ticking on the implementation of NIS, some member states are in a better position to implement the directive than others. For instance, in October 2016, the UK government launched the country's first National Cyber Security Centre, which is part of GCHQ and will bring together CESG – the information security arm of GCHQ – the Centre for the Protection of National Infrastructure, CERT-UK and the Centre for Cyber Assessment to form a single organisation that will simplify the country's approach to cybersecurity. Although it is not clear how far the UK will need to comply with the new rules when the country withdraws from the EU.

Other member states are playing catch-up and having to drag companies into line. "I was in Belgium with a big company recently and the Belgian government had told this company that it was a critical business for the country, but the company argued it was not," says Wouter Wissink, senior information and network technology specialist, risk engineering services for Continental Europe at Chubb.

"The company finally accepted it was a critical business and, in this instance, I've seen a positive impact already because this company has decided to separate its SCADA [supervisory control and data acquisition] network from the internet. It's good that at least companies are starting to think about it, and will have to report to authorities what they are going to do and how they are going to do it. This thinking will lead to a higher awareness in an organisation and that's very positive."

Although question marks remain around how the new directive will be precisely implemented, no one doubts that NIS will have a positive impact on Europe's ability to thwart would-be hackers.

Intelligence-sharing among companies and member states on the nature, extent and methods of attack will undoubtedly enable businesses to bolster their cyber defences. It will not stop attacks completely, but it should help to minimise the damage caused. ■

Key points

Face the facts
Cybercrime is growing and the chance of your company being targeted is high.

Change with the times
The chance of the attack being successful is also increasing, which is why many companies are shifting their strategic approach from simply protection, to detection and reaction.

Essential service providers take note
If a government considers your business to be a provider of essential services and/or digital services, you will need to comply with the new network and information security requirements outlined by the NIS Directive.

Be ready for the new rules
There is currently a grace period of a year and a half while national governments decide how to interpret and implement the terms of the directive, but cyber experts say that businesses affected by NIS should start preparing now.

Know when to declare a breach
One challenge for companies that fall under the remit of NIS is determining what constitutes a breach under the terms of the directive. Experts advise creating a breach escalation matrix so that you can make an informed decision about when to declare a breach.

55%
Growth in employee-targeted spear-phising campaigns in 2015

469
Days taken on average to uncover a cyberattack in the MENA region

Get in touch

If you would like to discuss any of the issues raised in this article, please contact Nick Bellamy at NBellamy@chubb.com

Illustration: hitandrun @ Debut Art

Travel safe

Wealthy travellers are targets for thieves, right from the taxi rank to the hotel room

When you own jewellery worth millions, taking a €100,000 engagement ring or watch abroad is not out of the ordinary. But wealthy individuals are particularly vulnerable when travelling. So what can those with highly valuable personal possessions do to mitigate the of risk of theft when they are on the move?

"Planning transport links ahead of arrival can minimise time spent hanging around, perhaps attracting unwanted attention. Some clients even have very good costume jewellery made to look like the real item and keep the real item in baggage to try and protect it while travelling," says Chris O'Rourke, European signature manager, personal risk services at Chubb.

When staying in hotels, it is also advisable to secure expensive jewellery inside the hotel's main safe, rather than the small safes often found in hotel rooms, adds Chris. "The safe in the office of the hotel will be far more robust and there are other layers of security, including staff, that make unauthorised access even more difficult." Wealthy individuals using this tactic should also ask who has access to the safe and whether access is properly monitored.

When an item is stolen or lost on holiday, travellers become acutely aware of its value. It is therefore important to stay on top of current values, says Chris. "If you have an insurance policy where an item is specified, it's a good idea to get it regularly valued, as jewellery values can increase significantly year on year. At Chubb, we work to an 'agreed value', meaning the client has certainty around the financial consequences of a claim. We also provide protection against underinsurance so that if the agreed value is not enough following a claim, but your jewellery has been valued in the past two years, we will pay above the agreed value." ■

Photography: Getty

I am your data. Protect me.

I sit in the cloud.

I am in your databases and devices.

I grow by 100 terabytes every day.

I am millions of confidential records.

Names, addresses, bank account details.

I want a particular kind of protection and level of service that comes from decades of experience insuring companies against the risk of network breaches and compromised data.

Not just coverage. Craftsmanship.℠

Not just insured.

Chubb. Insured.℠

chubb.com/uk

CHUBB®