CHUBB®

2017 Issue 2

# Progress


## Social engineering

The con is on, with criminals increasingly impersonating executives

**Drones take off**
But do commercial operators understand the risks?

**Stage fright**
How event organisers can be prepared for all eventualities

**Start-ups**
What should budding Zuckerbergs have on their minds besides strategy?

# Welcome

People around the world are increasingly starting to expect the unexpected after the events of recent years. I hope this will make the work of risk managers easier as they push the contingency planning agenda within their organisations. Alongside changes in geopolitical risk, which we assess on page four, many companies have also been left spinning by rapid advancements in technology. Unmanned aerial vehicles is one area already transforming the way businesses operate. On page 10, we explore some of the risks faced by innovative commercial operators.

Technological progress has also created new tools for criminals, but it is an old-fashioned type of fraud that is seeing a resurgence right now. As we examine in our cover story, there has been a spike in the number of criminals impersonating company executives for fraudulent gain. Turn to page six to find out what to look for and the preventive measures you should have in place. Of course, risks such as this might not be the top concern of entrepreneurs as they battle to gain a foothold in business - on page 14, we consider what risks start-ups should make time to manage. Meanwhile, our infographic on page 24 offers a cautionary tale of having the wrong type of insurance in place.

As ever, we are happy to give advice on how best to mitigate and manage risks in your sector, so please do get in touch using the contacts listed in each article.

Andrew Kendrick
Regional President, Europe
Chubb

CHUBB®

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

Chubb 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. Full details can be found online at https://register.fca.org.uk/

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

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 Matt Williams
Account Director Charlotte Tapp
Creative Director Ben Barrett
Managing Director Claire Oldfield
CEO Martin MacConnol

'wardour'

Cover illustration: Jacquie Boyd/Debut Art

**4** New world disorder
Geopolitical risk can seem intractable in this volatile world, but it can be managed

**6** The hustle
If your boss called and asked you to transfer money, would you do it? Employees are increasingly the weakest link in fraud prevention

**10** Flying without wings
Unmanned aerial vehicles are being used in ever-more commercial settings, but what are the risks?

**14** Starting up
Born out of risk and fast-paced by nature, start-ups can lose sight of their liabilities. But what are the common pitfalls?

**17** The data deadline
With the clock ticking on the deadline for new data regulations, we set out the steps companies should be taking to prepare

**18** The show must go on
A cancelled event can cost organisers millions, but there are many ways they can avert disaster

**22** Whisky galore
Thieves are targeting cargo ships with zeal, and food and drink is top of their lists

**24** Plugging a cash leak
We look at what a Local Education Authority did to incur a hefty bill for an environmental clean-up and how it could have held on to its money

**27** Critical benefits
How employers in France are responding to the pressures facing people with critical illness

**30** Wake-up call
When the WannaCry virus was unleashed in May, the importance of cyber-specific insurance became startlingly apparent

10

14

18

# New world disorder

Geopolitical risk can seem intractable in this volatile world, but it can be managed, say Chubb's **Piers Gregory**, Head of Terrorism and Political Violence, and **Murray Ross**, Head of Wholesale Political Risk and Credit

Global instability and uncertainty have reached new and dangerous levels in recent years. It was in this context that we led a panel discussion at Chubb's Multinational Risk Forum in March on how organisations can identify, quantify and manage their exposures along the ever-changing geopolitical risk spectrum.

Terrorist attacks have intensified and their methodology and targets have grown more unpredictable. In Europe and the US, the rise of populism and the near-collapse of the old order have escalated geopolitical risk for businesses, lenders and investors.

In the past, terrorism risk (in a risk transfer context) was primarily about the destruction of property and associated tangible assets, and was more common in unstable regions. But, following the murderous attacks in Barcelona, Manchester, Berlin, Paris, London and New York, the scope of terrorism risk has changed. The ideology of terror groups is now diversified across multiple territories and the scope of their targets has increased. We have seen the threat emerging in different ways, with lone-wolf attacks perpetrated by individuals – and, as such, more difficult to police – becoming more frequent.

> "The ideology of terror groups is now diversified across multiple territories and the scope of their targets has increased"

## Business interruption

From a purely business perspective, the challenge to companies is understanding how that type of incident could affect their revenues. While in the past companies might have focused on insuring against the impact of a large bomb, today one of the biggest risks is business interruption, when transport links are closed down and normal operations suspended. That brings the supply chain into focus and, with that, the concept of 'non-damage business interruption'.

The insurance market is moving fast to come up with products that will respond to the changing nature of geopolitical threat, which has placed the market under pressure to innovate and consider this business interruption risk element. There are many more products available on the market now that seek to address new types of threat. Loss of attraction, for example, is an extension to business interruption that covers a policyholder against losses caused by the destruction of property close to their own, while prevention of access would kick in when police seal off an area, for example.

However, insurers are proceeding cautiously so as not to lose sight of accumulation risk and the need to understand and control this. For clients, a clear understanding of the protection offered by policies is important, and improvements in wordings provide more clarity and certainty about how the policy will respond to an event.

For example, Chubb provides optional extensions for terrorism and political risk to traditional property damage business interruption (PDBI) policies. This gives buyers peace of mind around claims payment because it bundles a number of perils with the one carrier, minimising gaps in coverage.

We are also in the process of updating our risk engineering proposition to include a more robust review of terror and political violence (PV) risk. This allows our clients to more actively manage this risk in terms of both assessing physical onsite security and possible gaps in protection, as well as the location risk, therefore identifying assets that may be within the immediate vicinity of our clients' premises that could raise the profile of terror or PV risk. This is not standard within our market.

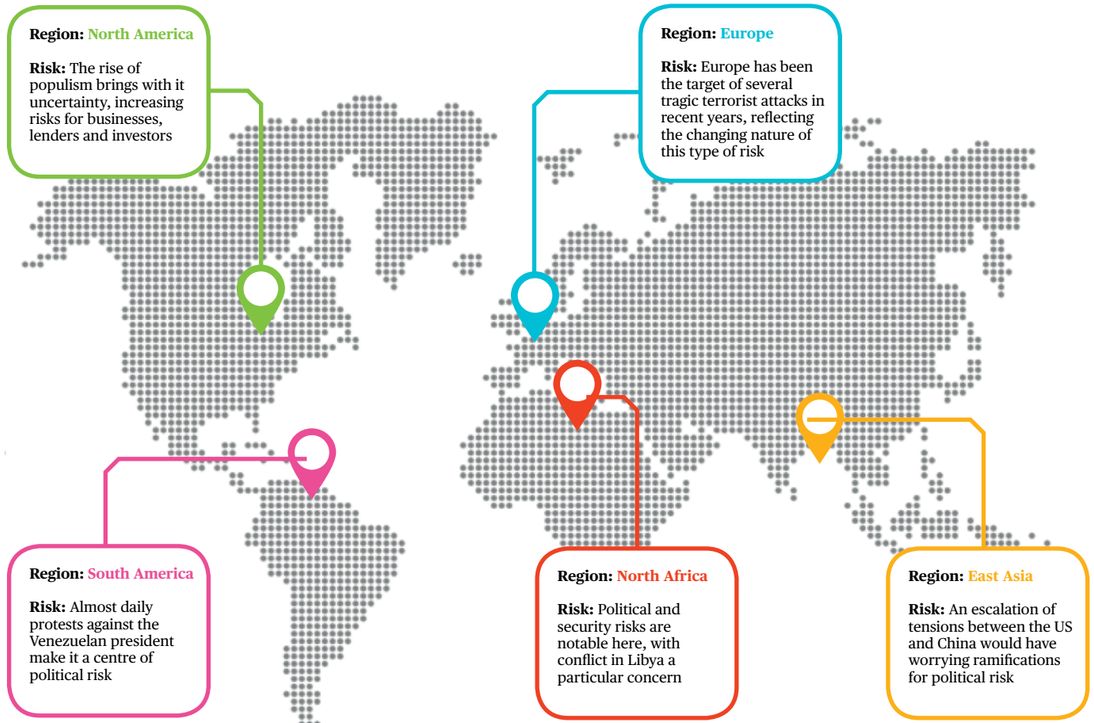



Illustration: Peter James Field/Agency Rush

On the political front, the risk landscape is equally unpredictable. Definitions vary but, unlike terrorism, political risk usually refers to the potential for losses resulting from government actions. In its simplest form, it can mean the risk of an investor, lender or exporter not being paid; it can also relate to expropriation or freezing of assets or inconvertibility of currency, for example.

The panel agreed that the rise of populism in different countries has triggered widespread uncertainty. Populism frequently brings protectionism with it, as has been hinted at in the US. Similarly, events in East Asia have the potential for widespread political fall-out and, once the scale of the US–China power struggle becomes apparent, worrying implications could emerge from a political risk point of view.

Another example of the problems that populism can suddenly spark is the recent row between the Netherlands and Turkey. When the Netherlands refused two Turkish politicians permission to enter the country, Turkey said it would react in the harshest possible way. A completely innocent, benign Dutch investor in Turkey could easily be impacted in circumstances like this, and an increase in these kinds of skirmishes looks likely.

Risk managers attending the panel discussion agreed with this analysis, highlighting some of the many challenges that they face. One said that the multi-faceted nature of political risk makes it hard to manage; another agreed, adding that colleagues in different business units each have their own ideas of what political risks they are exposed to.

## Receptive to risk

Chubb and other insurers also grapple with the fast-moving nature of political risk, so we are not always able to cover every political risk that customers enquire about. Sometimes, this may be due to cover being requested late in the day – for example, with the queries that came in suddenly from Russia after it intervened in Ukraine. Generally, though, multinational businesses, lenders and investors that think ahead will find a receptive political risk insurance market that can offer the limits and coverage they need. ■

### Get in touch

To find out more about how Chubb can help organisations mitigate political and terrorism risks, please email Piers at piers.gregory@chubb.com or Murray at murray.ross@chubb.com. Alternatively, speak to your local Chubb office

# The hustle

In a world where computer systems are ever more secure, it is often people and not technology that are vulnerable to criminals, writes **Paul Rubens**

Your CEO is away on holiday, but he emails you to say that a top-secret deal has finally come together. He needs you to arrange a bank transfer for a large sum right away – the whole deal will fall through if the payment is delayed. And one more thing: it is all confidential so you are not to mention it to anyone in the office until he gets back on Monday and the deal is complete.

Scenarios like this have become increasingly common over the last few years, and they all have one thing in common: they are all variations of a type of crime known as social engineering fraud, and they can lead to substantial financial losses for the victims.

The idea behind social engineering is simple: a criminal gets an employee to believe they are dealing with someone legitimate – their supervisor, their boss or perhaps a customer – and persuades them to make a payment. By the time the fraud is discovered the money is long gone and is usually not recoverable.

This type of fraud has become a significant problem throughout the world. Criminals using one particular social engineering attack – sending out emails asking employees to change the bank account details to which certain payments are made – resulted in average losses of over £100,000 (€ 109,000) per incident across 90 different countries, according to Trend Micro research. And some countries are affected more than others, perhaps because international fraudsters have difficulties with some languages. For example, 2% of companies in France and Norway have been affected by social engineering fraud, but that figure rises to 9% in the UK.

> "A fraudster can carry out digital reconnaissance before making contact"

One reason that social engineering fraud has been on the rise is that it is relatively easy to carry out, according to Anthony Wright, UKI Senior Financial Lines Underwriter at Chubb. "When it comes to security in many organisations it is individuals that are the weakest link, and social engineering fraud is all about duping individuals," he says. "If you don't have controls in place to try to prevent social engineering fraud, you have no chance if someone targets you," he adds.

The most basic form of social engineering involves sending out large numbers of identical emails to organisations requesting that future payments to a common supplier (such as an electricity or phone company) be made to a different bank account. This type of fraud may be relatively simple to spot. That's because the email may contain blatant spelling mistakes or grammatical errors that make it obvious that it doesn't come from the company it purports to be from, for example.

But more sophisticated attempts at social engineering fraud are far harder to spot. A fraudster targeting a particular company can carry out digital reconnaissance before making contact. He could, for example, watch a video of the CEO of a company making a presentation on YouTube to get an idea of how he speaks and what kind of mannerisms he has. The fraudster could then go further, choosing a suitable employee from the company's website, and finding out personal details about them from Facebook, LinkedIn and other social media sites.

"Using those sources, a criminal can build up a profile of 'Tim from Accounts': he has been at the company for five years, he plays golf and he reports to Mandy," explains Graham Hollingdale, a UKI Financial Lines Development Underwriter at Chubb. "Then the fraudster can establish when the CEO is on holiday (perhaps from Facebook posts), impersonate the CEO, call or email Tim, talk about golf and come up with a believable story about why a payment needs to be made and Mandy mustn't be told."

## Flattering employees

Typical social engineering tricks involve techniques as simple as flattery. "You've been at the company for five years, so I know that I can trust you to make this important payment confidentially," is the type of social engineering that a fraudster may attempt to use.

"A fraudster may then add a sense of urgency to the transaction by saying that there is a deadline for the payment and the deal will collapse if the payment is later, or something like that," says Graham. "That's designed to make the employee feel that they may be responsible so they may not take the time to check that the transaction is legitimate, or bypass usual processes before making a payment."

Social engineering can be made even more effective if a criminal has hacked into a corporate email system and has access to internal communications between managers and other employees, explains Anthony. "Fraudsters can blast out thousands of emails a day in the hope of fooling someone – and ▶


Illustration: Jacquie Boyd/Debut Art

there is always someone who will be duped on any given day if you send enough emails out - but what we are seeing is fraudsters spending more time doing research. They will read email exchanges between specific people in a company and then copy the style of these exchanges."

However, not all social engineering fraud involves tricking employees into making payments, warns Anthony. Often they can involve property rather than money. "One social engineering fraud that I came across that stands out involved camera equipment. A company that is a supplier to a broadcaster received an order form supposedly from the broadcaster, and an employee was persuaded to deliver a large amount of expensive equipment to a location," he says. "In fact the broadcaster had never worked at that location and had never ordered the equipment.

A similar fraud involved someone calling a company while purporting to be a client and collecting goods which were never seen again."

One way to mitigate the risk of social engineering fraud is through insurance, but it is important to understand what type of insurance is required, according to Anthony. "This is an area of huge misunderstanding," he says. "Some companies think that if they have been tricked by an email or made an electronic payment that this is cybercrime, but cybercrime or computer violation insurance doesn't cover social engineering. What you need is crime insurance."

What's interesting is that, while this type of insurance is relatively inexpensive, many companies don't bother with it, according to Bryan Banbury, the Managing Director of insurance broker Russell Scanlan. "Many companies install an intruder alarm, CCTV,

> "Insurance companies expect customers to put processes in place to protect themselves"

bars on their windows and so on for their physical security, but they still have insurance as a back-up. But when it comes to social engineering fraud, they don't have the back-up of insurance."

## Crime insurance

The good news is that modern crime insurance policies tend to be very broad, covering financial loss rather than specific crimes. That means that a business is likely to be covered even if an employee is tricked using social engineering into transferring money out or even handing goods over to fraudsters voluntarily. But Graham points out that most insurance companies will expect customers to put processes in place to protect themselves from social engineering fraud. Implementing these measures can (and demonstrably has) reduced the risk of some types of social engineering fraud significantly. "When you buy crime insurance, you are likely to be given best practice guides which can be sent out to employees," he says. "Certain controls can be very helpful, but with social engineering there is always the risk that a human will be fooled."

Typical best practices include instigating a call-back procedure requiring employees to call the individual in an organisation who has purportedly asked for a payment to be made; requiring two directors to authorise payments; and only making payments to bank accounts that are on an approved list. Graham adds that in some cases it may be prudent to impose even tighter controls - for example in branch offices of businesses with just a few employees, or overseas offices, which can be particularly vulnerable. "That is especially true in certain parts of the world where people are less likely to challenge an instruction which appears to come from someone in authority for cultural reasons. Rather than question a superior they are more likely to simply process the request." ■

**9%**

of companies in the UK have been affected by social engineering fraud, while 2% have been hit in France and Norway


## Three common types of social engineering fraud and how to protect against them

**1. 'Fake CEO' fraud**

Before making any payments, employees should always:

- Call back the director who has purportedly given the instruction to make a payment using the number in the corporate phone directory (and not on a phone number supplied in an email).
- Verify the payment request with another director, and check the bank account to which the payment is to be made is on an approved list.

**2. Fraudulent payment and fund transfer requests**

Employees should always:

- Refuse to give or accept payment instructions by phone or email.
- Accept payment or transfer requests only if they are in writing, on company headed paper.
- Verify all requests with a call back procedure to a known contact, to confirm authenticity.

**3. Email scams and requests to change bank account details**

Employees should always:

- Check that the sender is on an approved list of contacts, and check for spelling mistakes.
- Click on the sender s email address in the message to ensure that it is not masking a bogus email address.
- Use a call back procedure to a known contact to verify that the email is genuine.
- Check the client file for previous requests to amend bank account details or send large sums to new accounts.

**General security controls**

- Maintain an approved list of suppliers and vendors, including key contacts with email addresses and telephone numbers.
- Ensure suppliers and vendors know that any requests to change bank account details should be sent in writing on company headed paper, signed by an approved person.
- Have a dual-control procedure in place when appointing new suppliers to prevent fictitious vendor fraud.

# Flying without wings

**Drones are no longer just the playthings of technology enthusiasts. Today, the commercial market is set to take off in a big way, but with regulators still catching up, Stuart Collins assesses the risks**

Photography: Rex

Unmanned aerial vehicles (UAVs), or drones, might seem like a novelty, used to spy on celebrities, or to film Hollywood blockbusters and sporting events like Formula One races. Yet these devices are finding an increasing number of commercial and civilian applications.

In Africa, UAVs are saving lives. They deliver medicines, blood and vaccines to people in remote communities - for example, UNICEF trialled a UAV service in Malawi that transports blood samples from newborn babies from a clinic to a laboratory.

Scientists are using UAVs to study volcanoes, monitor shrinking ice caps, and map pollution spills and harmful algal blooms. They are being employed to fight fires, prevent crime, locate earthquake survivors, and even to prevent shark attacks in Australia.

The UAV market is growing rapidly. Research firm Markets and Markets expects the global drones sector to be worth US$21 billion (€18 billion) by 2022.

To date, much of the growth has been in the consumer space. Commercial applications have generally been small scale and experimental, but that may be about to change.

Between now and 2020, Goldman Sachs forecasts a US$100 billion (€84 billion) market opportunity for drones, helped by growing demand from the commercial and civil government sectors, which it expects will spend US$13 billion (€11 billion) on drones over the next three years.

"What we see today is just the tip of the iceberg. New applications for UAVs are emerging all the time, while almost every week we see new innovations," according to Mark Adams, UKI Senior Underwriter for Aviation at Chubb.

"At present, the commercial UAV market is mostly populated by small specialist service providers," explains James Gadbury, COO of UAV Protect, a specialist drone insurance provider from Prospect Insurance Brokers. "Large companies have tended to buy in UAV services rather than invest in their own equipment and training, but we expect these companies will develop their own UAV capabilities in coming years, especially as the regulatory environment evolves," he says.

Agriculture, mining, energy and construction are all expected to use UAVs to perform hazardous or repetitive tasks, like crop-spraying, prospecting or surveying. The shipping industry, for example, is beginning to use UAVs to survey vessels and inspect cargo holds, fight piracy and smuggling, as well as to make ship-to-shore deliveries.

## Compliance challenge

For companies looking to use UAVs, there are a number of regulatory, operational and legal considerations.

Regulatory compliance is probably the biggest challenge for companies using UAVs, according to Raymond L Mariani, an attorney at New York-based law firm Murray, Morin & Herman. In the US, for example, companies face three layers of regulation: federal, state and city laws, he explains.

It is difficult to generalise about UAV requirements, according to Mark. UAV regulation is changing all the time and requirements vary greatly by country, he says. "Operators should seek out local advice and expertise, and at least refer to their national civil aviation authority."

Unlike commercial aviation, there are no international rules on UAV safety and liability, although the International Civil Aviation Organization (ICAO) plans to publish UAV standards in 2018. At present, there is also no single set of EU rules governing UAV use, and Europe remains a patchwork of differing national rules.

Generally speaking, most countries require commercial UAV operators to obtain authorisation or a licence to operate, especially when flying in urban areas, close to buildings or flying beyond the line-of-sight. Each national authority applies its own safety restrictions, typically based on the weight and intended usage of the UAV. These typically include requirements to stay within a maximum flying altitude and for UAV pilots to undergo training.

In August 2016, the Federal Aviation Administration (FAA) introduced dedicated regulation for US commercial UAV operators under Part 107 of the Federal Aviation Regulations. While a step forward, the regulations include significant restrictions on the use of UAVs, such as a requirement to fly within the line-of-sight, explains Raymond.

Yet many promising UAV applications - such as crop-spraying, delivering cargo or ►

> "UAVs are being employed to fight fires, prevent crime, locate earthquake survivors, and prevent shark attacks in Australia"

surveying remote pipelines – will suit vehicles that fly beyond the line-of-sight, or even those that fly autonomously.

## Flying taxis

While regulatory developments have opened the market for lightweight UAV usage within line-of-sight, rules are very restrictive for larger and autonomous UAVs. But pilotless aircraft are being developed to transport cargo and even take passengers. One company already plans to test an autonomous flying taxi service in Dubai by the end of the year. But such ventures face significant regulatory hurdles.

According to Raymond, the FAA is taking a cautious, safety-driven approach to UAVs and is unlikely to relax rules for larger and beyond line-of-sight uses any time soon.

"Restrictions will not be lifted quickly. The FAA will want to get much more comfortable with UAVs' sense and awareness capabilities, which enable them to avoid collisions with other aircraft, people and objects," he says.

One big challenge is to manage the integration of UAVs with civilian airspace used by passenger jets, especially as UAV traffic grows. The number of incidents involving UAVs at London airports rose to 36 in 2016, of which 10 were classed as a serious risk of collision.

In Europe, there have been 606 safety incidents (such as airspace infringements) involving UAVs over the past five years, of which 37 have been classified as accidents, according to the European Aviation Safety Agency (EASA) *Annual Safety Review 2017*.

Safety concerns mean that small UAVs must stay below 400ft (120m) in the UK, while large UAVs are only allowed to fly in special test locations that exclude other airspace users.

Similar rules exist in other European countries. New rules introduced this year in Germany, for example, restrict UAV usage to a height of 100m without special permission, while units weighing in excess of 250g cannot be flown over residential areas.

The EASA is currently consulting on the regulation of small drones in the EU. The rules will cover technical and operational requirements, such as when and where a UAV can be flown, registration and pilot training.

One possible solution will be the creation of UAV lanes or corridors, something that is being explored by authorities in the UK, US and Singapore. Techniques to disable UAVs are also being developed, ranging from hunter-killer UAVs to specially trained birds of prey. Developments in technology could also improve safety in the longer term, believes Mark. For example, better collision avoidance systems are needed, as is improved cyber security, he says.

> "A shift to larger, more valuable UAVs, operating in urban areas and beyond the line-of-sight, would clearly lead to much larger liability and exposures"

Other than regulatory compliance, the principal risk of operating a UAV is that of a collision, which can result in the loss of the UAV or, even worse, bodily injury or damage to third-party property. The value of most UAVs is relatively small, but more complex and larger drones can be worth upwards of US$500,000 (€420,000), according to Mark. And as they get larger and find more sophisticated uses, such as 3D mapping, values are likely to climb, he predicts.

More concerning is the potential to cause bodily injury or damage to property on the ground. The risk of a collision with an aircraft is an obvious concern, as is flying over crowds or urban areas.

Drones have crashed at several big sporting events, including the US Open, while another crashed at the 2016 Skiing World Cup, narrowly missing skier Marcel Hirscher.

According to Mark, technical faults are a common cause of UAV accidents, but human error is also a factor. "Safety remains a concern. Even with trained pilots, UAVs can still fail or stray into sensitive locations or urban areas," says Mark.

To date, claims seen by insurers have been relatively low value (such as damage to parked cars), reflecting the low value and lightweight nature of most UAVs. However, as they become more complex and heavy, exposures are expected to increase.

"For now we mostly see smaller UAVs of low value and restricted use. But a shift to larger, more valuable UAVs, operating in urban areas and beyond the line-of-sight, would clearly lead to much larger liability and exposures," according to James.

As UAVs become more prevalent, insurance is likely to become an important mechanism to compensate for third-party damage. While passenger aircraft are required to carry aviation insurance, this is not the case for UAVs in all countries.

Commercial UAV operators in the EU are required to hold third-party liability insurance with a limit of no less than €1 million. But UAV operators in the US, for instance, are not currently required to do so, explains Raymond. Insurance regulation in the US is state-based, and while some states (like California) have proposed mandatory insurance, these have been rejected, he says.

The Unmanned Aerial Vehicle Systems Association advises all commercial UAV operators to purchase appropriate third-party insurance. It is concerned that too many UAV operators do not have appropriate third-party liability insurance in place, while many of them rely on public liability insurance, which typically excludes aerial work.

Best practice and contractual requirements are already driving the need for UAV insurance, according to James. "Companies typically require vendors to demonstrate that they hold appropriate insurance," he says.

## Insurance considerations

Operators need to be careful when purchasing insurance, advises Mark. Almost without exception, aviation risks are excluded from public liability and general liability policies, he explains.

According to Raymond, commercial operators would be wise to purchase general aviation cover or specialist UAV insurance. "The growth in the UAV market has been accompanied by exclusions," he says. "General liability insurers do not look to pick up this type of exposure and have added specific exclusions for aviation risks to general liability policies."

The need for appropriate cover has also caught the attention of regulators. The UK's Civil Aviation Authority (CAA) recently clarified its insurance requirement, specifying the need for commercial UAV operators to purchase aviation cover.

In response to demand, the aviation insurance market has developed insurance specifically for UAVs. This is a specialist area and has not been an easy product to develop, explains Mark.

"UAV insurance combines a number of areas of aviation and general liability expertise. At Chubb we have taken a measured approach to UAV insurance, and aim to provide good cover in a difficult and changing regulatory and technical environment," concludes Mark. ■

### Privacy and cyber risks

In addition to risks associated with collisions, UAV operators face other liabilities.

Privacy has emerged as a big issue in recent years. The Information Commissioner s Office in the UK warned in 2014 that commercial drone operators are subject to data protection laws and would need to conduct a privacy impact assessment.

Unintentional privacy breaches are a real risk for commercial operators, for example when they are filming in public or surveying buildings in public, explains Mark.

There have already been lawsuits in the US around privacy, as well as noise and trespass, according to Raymond. "While there are only a few cases at the moment, we will see more over time," he says.

Cyber security is another consideration for operators. Ground-to-air signals can be deliberately jammed or interfered with, while UAV cyber security has shown to be wanting. Security researchers have hacked into UAVs, including high-end drones used by the police and industry.

Operators may also be exposed to professional liabilities, according to James. For example, errors or omissions in data sourced by a UAV – such as in 3D mapping – could result in a financial loss to the client, he explains.

Photography: istock

# Starting up

Born out of risk-taking and fast-paced by nature, start-ups can lose sight of their liabilities. But what are the common pitfalls? **Andrew Pring** reports

Start-up entrepreneurs are inspired, often brilliant people. Fuelled by boundless optimism, they focus relentlessly on the big picture – the vision of success that makes the long hours and sacrifices all worthwhile. But as with any newly emerging life, there's a vulnerability about entrepreneurs too.

The intensity of the start-up process is a dangerous time for a budding Zuckerberg or Bezos, often blinding them to unglamorous but fundamental aspects of business. In these early stages, the need to attract investors, assemble teams, find offices and win customers dominates thinking, and many basic business risks are just not factored in to the plan. Sadly, such oversight can rebound disastrously on the start-up, derailing its progress, perhaps terminally, before it has even properly begun.

Within the booming technology sector, these basic business risks are everywhere. Start-ups can see their products or services fail, leaving them contractually exposed to their customers. Major disruption can arise from something as basic as building contractors cutting through power cables. But most embarrassingly of all for an infotech company, it can find itself the victim of a cyberattack, which could cause havoc, both for the company itself and its customers. It may even unknowingly become implicated in tax evasion and money laundering by criminals or terrorists. The reputational damage for a company supposed to be expert in IT could be catastrophic.

Defusing these problems, and there are many others like them, is vital for the future of the technology sector in Europe. The sector is hot, and countries are competing hard to attract innovative start-ups, offering a range of services and tax breaks as inducements. But for the next Amazons and Apples to flourish, create jobs and inject entrepreneurial dynamism into their host economies, they need to overcome a sometimes blinkered approach to business.


Illustration: James Taylor

> "The intensity of the start-up process is a dangerous time for a budding Zuckerberg or Bezos, often blinding them to unglamorous but fundamental aspects of business"

Marcellien Breedveld met many start-up entrepreneurs when she worked as Ideation Manager at UtrechtInc, a Dutch business incubator set up eight years ago by the Ministry of Economic Affairs to bring research knowledge to the market and make a social impact. It has supported 157 start-ups, with a 63% success rate, and Marcellien, who worked there until May, opened the eyes of many business-innocent entrepreneurs during that time.

"Entrepreneurs are very enthusiastic about their product. They're generally young and tend to be very optimistic. But innovation takes a long time to get to market so it eats up an entrepreneur's time, and there's a lot of chaos and uncertainty in this period. Insurance and risks are not their highest priority. They're more concerned with customer-facing issues than anything else, but then the money runs out!"

UtrechtInc's role is to make sure things do not get anywhere near that stage. "We make sure they are linked to financial experts who offer a full range of advisory services," says Marcellien. "In our experience, failure is generally down to lack of customers and poor team performance more than internal, operational matters, such as lack of insurance. But we definitely want entrepreneurs to receive the best advice possible so they can make smart decisions on those operational risks."

Charles Bethoux, Technology Underwriting Manager for Continental Europe at Chubb's Paris office, concurs with Marcellien's assessment of start-ups. "They are often very fast-moving and free-wheeling, with a lack of internal controls or procedures in the early stages. They also often have a high staff turnover and vetting is not always carried out properly. This makes them vulnerable to crime and fraud, and rogue employees and third parties can exploit this."

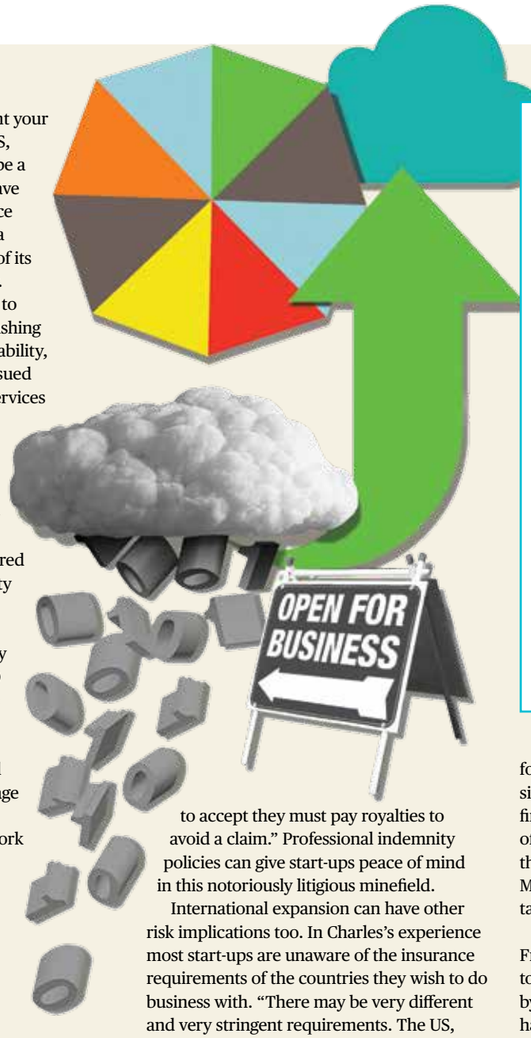
## Avoiding the traps

Financial loss risk comes in many forms, but one area that causes particular concern for tech start-ups is contractual liability, says Charles. "Clients want their business partners to take out financial loss insurance. It's often written into the contract and the client – particularly if they're a big company – will seek to impose as much liability onto their supplier as possible. These terms can be quite onerous, leaving the supplier responsible for making good any loss incurred by the company. And as a start-up, they'll be in no position to resist and will have to accept the terms if they ▶

want the business. If you want your software distributed in the US, for example, or you want to be a supplier to Amazon, you'll have to comply with their insurance requirements, which means a company can pass on a part of its own liabilities to the supplier.

"We encourage our clients to manage their exposure by pushing back and not accepting full liability, and the recommendations issued by our Chubb Engineering Services team or by their insurance broker can help them."

Charles and his team still regularly see the insurance element missing from a start-up's business plan. "They often think everything's covered by a standard General Liability insurance policy, but that's far from the case." Only a Professional Indemnity policy (also called Technology E&O) could respond to most of the technology related financial injury claims. In addition to financial loss and contractual liability, the insurance coverage should address privacy, reputational injury and network security claims exposures.




## Originality

Other regularly overlooked start-up risks involve intellectual property and international expansion. "It's very important for start-ups to protect themselves against intellectual property rights infringement claims. With new technologies, the same ideas can occur in other parts of the world so companies need to check this, which can be difficult and laborious, especially in the field of copyrights and computer codes," says Charles.

"And there's another problem too – rivals may seek to prevent a company entering its territory by claiming intellectual property infringement, and sometimes start-ups have to accept they must pay royalties to avoid a claim." Professional indemnity policies can give start-ups peace of mind in this notoriously litigious minefield.

International expansion can have other risk implications too. In Charles's experience most start-ups are unaware of the insurance requirements of the countries they wish to do business with. "There may be very different and very stringent requirements. The US, for example, is a highly regulated market and start-ups wishing to operate or sell there would need to seek US exports insurance extensions or US admitted insurance for their local staff and their business. Sorting this out can delay expansion plans."

Even with the right insurance protection in place, success is clearly not guaranteed, so directors' and officers' (D&O) insurance is another vital protection. "Bankruptcy risks are very high in the first three years of any start-up, and particularly when the founders are focused on the technical side of the business and not so much the finances," says Charles. "Founders often offer their homes as loan security, so they're very exposed if the business fails. Many companies ask their suppliers to take out D&O cover."

Christophe Gautié, a broker with the French firm Apollo, offers specialist advice to infotech start-ups and is often struck by the inadequacy of their cover. "Many have just gone to their domestic insurer and then when something goes wrong, they find themselves badly placed. It's far better if they're insured properly right from the start." ■

### Key messages

1. Start-ups should focus on day-to-day business risks as much as product innovation and marketing, and insure accordingly.
2. Insurance can cover loss of revenue and profit if a cyberattack disrupts business.
3. Premiums to cover start-up issues can be surprisingly inexpensive – professional indemnity (PI) is often cheaper than car insurance.
4. Arrange cover before embarking on overseas expansion. Other countries' legal requirements may differ greatly from those of the country of origin.
5. Potential infringement of intellectual property rights needs extra vigilance, particularly in foreign markets. PI insurance can protect against inadvertent breaches.
6. Comprehensive insurance packages that protect against most start-up risks are available.

### Get in touch

For more information on Chubb's services for technology companies, contact Charles Bethoux at cbethoux@chubb.com

"With new technologies, the same ideas can occur in other parts of the world so companies need to check this, which can be difficult and laborious, especially in the field of copyrights"

# The data deadline

With the clock ticking on the introduction of new data protection regulations, we ask what companies should be doing to prepare

The name of Europe's new data regulation might not be eye-catching, but the potential fines certainly are. When the General Data Protection Regulation (GDPR) comes into force in May 2018, companies found to be non-compliant could stand to lose 2–4% of their global turnover. Any company handling personal data of EU residents will be affected, even if they are based outside the region. Yet, a global survey by Dell in October 2016 found that 97% of companies do not have a plan in place to meet the new requirements.

The GDPR essentially builds on existing data protection rules, taking existing privacy rules but enhancing regulatory requirements. A good example is the enforcement regime, which will give regulators powers to levy much bigger fines for non-compliance. Another big change is a requirement to notify regulators within 72 hours of a security breach. The rules around collecting consent to use individuals' data will also change and privacy policies issued to users must provide more information to explain exactly how data is going to be used. Consumers will get new rights to change preferences, be forgotten and move their data between service providers. Some organisations will need to appoint a data protection officer and carry out privacy impact assessments before engaging in higher risk projects.

Looking ahead to May, here are some of the basic steps organisations should take to prepare, but this is a significant piece of legislation with wide-reaching effects, so this list is by no means exhaustive.

**Data mapping** – one of the first steps any organisation should take is to work out what data it holds and how it is being used. Andrew Dyson, Partner at law firm DLA Piper, explains: "Work out what data you've got, where it's sitting, who's using it and how it's being managed. In tandem with that, work out where there might be gaps – where you might be collecting data but you don't have a proper privacy policy, where you might not be getting the right consent, or where you might be relying on a third party to help manage your systems but don't regulate data under your contract."

**Culture change** – ensure that key individuals take ownership of compliance and understand the impact of GDPR throughout the business. Andrew says: "The organisation needs to build an accountability framework that you can use to demonstrate to a regulator that you know what your responsibilities are and have a clear plan and set of policies to effectively manage compliance within the business. That is really important to mitigate risk."

**Breach policy** – the 72-hour notification window is short, so it is important to have a strong cyber breach policy in place. Once a breach has been identified, organisations will need to determine whether it involved personal data, work out whether there is a duty to notify and then inform the regulator. Chubb's Regional Manager for Cyber Risks, Continental Europe, Kyle Bryant, says: "There are some easy things you can do to prepare, such as making sure that the lines of communication are strong. When we go in to advise clients, we ask how someone in their organisation would report an incident and do they need to shorten that time frame?"

**Privacy policies** – most privacy policies will need to be refreshed to meet obligations under the GDPR. "You'll have to give people more information about how you're looking to use their data, so rather than just saying 'we will use your data for marketing purposes', you will actually need to break down the activities to provide more granularity about what you are doing and who you will be sharing it with. It's about giving people a lot more transparency and control of what is happening with their data and what their rights are," says Andrew. Privacy must also be taken into consideration throughout the design process of new products or services.

**IT infrastructure and security** – users must have the option to change their preferences, to move their data and to be forgotten. That means technical teams will need to adapt the systems currently in place. Kyle also encourages clients to assess their security preparedness: "If the client has a low or moderate level of security, we like to move them up one notch. We need to try and improve them incrementally in order to prepare." ■

### Get in touch

Chubb provides a 24/7 hotline to help clients manage an incident. For more information, contact Kyle.Bryant@Chubb.com

# The show must go on

Whether it is a music festival or a business conference, cancelling an event can be costly. **Simon Creasy** finds out how organisers can be prepared

Photography: Shutterstock

When Dave Grohl, lead singer of the US rock band Foo Fighters, fell off the stage just two songs into a gig in Gothenburg, Sweden, in June 2015 it proved a costly mistake in more ways than one. Grohl, who suffered a dislocated ankle and snapped fibula, was forced to cancel the rest of the band's European tour at an estimated cost of US$10 million (€8 million) in lost fees and travel expenses.

It is not the first time something like this has happened. Events are regularly cancelled for all manner of reasons – a key artist gets sick, a piece of machinery breaks down or the weather refuses to play ball.

There are, of course, also tragic reasons for event cancellation, such as an act of terrorism or a musician who dies on the eve of a major global tour, as happened with Michael Jackson. Beyond the emotional devastation of such an event, the financial repercussions of these cancellations can be tremendous and result in payouts to customers and suppliers running into millions of euros.

But thankfully, today, most organisers of large events take out insurance so that, wherever possible, the show can go on. Event cancellation policies come under the umbrella of contingency insurance and primarily encompass cancellation, abandonment, postponement, re-schedulement or interruption of an event for a reason beyond the control of the organiser or the promoter.

This means that almost everything imaginable is insurable, including unpredictable factors, such as the weather. Insurance for bad weather at outdoor events usually kicks in when it becomes too dangerous for the event to go ahead, explains James Davies, Principal, Entertainment and Sport at Integro Group, an insurance brokerage that specialises in events. "This could mean covering anything, for example a cricket match with spectators given money back if the game is disrupted ▶

"Thankfully, today, most organisers of large events take out insurance so that, wherever possible, the show can go on"

**$10m**
The estimated cost of cancelling the Foo Fighters' 2015 European tour

**50%**
The refund given to 2017 'Y Not' festivalgoers after bad weather ended the event a day early

by the weather. The same principle would apply at tennis tournaments like Wimbledon and the French Open."

Indoor events can also be insured against adverse weather conditions, according to Francis Hernandez, Entertainment Manager for Overseas General Insurance at Chubb. "We covered a trade event on the east coast of the US and snow prevented people from attending. Even though the event wasn't cancelled, we paid out because half of the people weren't able to get to the show, which meant it wasn't able to fulfil its purpose. This is known as an 'enforced reduced attendance claim', whereby we reimburse the organiser for lost revenue because people can't attend."

## A new risk landscape

Adverse weather is one of the most longstanding and frequent risks event organisers face, but one of the newest and most devastating risks is terrorism.

In the aftermath of a terrorist incident, the financial implications are not the primary concern. But sometimes it is the threat of terrorism that stops an event from taking place, with big repercussions. One of the most high-profile examples in recent memory was the 2001 Ryder Cup, which was postponed after the American team decided not to travel to Europe following the 9/11 terror attacks.

The tournament was eventually pushed back a year, making it an even- rather than odd-year event, which had a knock-on effect on other events that were pencilled in for the following year. "That was possibly one of the most complicated sporting claims ever," says James.

A growing area of concern for event organisers in the UK is national mourning, according to Francis. "It's becoming more of a consideration with Prince Philip and the Queen getting older," he explains. "So any events connected to the royal family, such as Royal Ascot, or any London events that might be affected should streets be closed, such as the London marathon, would need to consider this."

He adds that event cancellation cover is deliberately kept quite broad, purely because it is difficult to predict what could cause an event to be called off; for instance, who would have forecast in 2010 that an ash cloud from an Icelandic volcano could have caused such widespread disruption?

"We have a named peril non-appearance policy that lists certain perils, such as death, accident or illness of an artist, travel delays, national mourning and venue damage, but then we have a last clause that says 'any other cause beyond the control of the insured'," says Francis.

Event cancellation insurance can be quite costly purely due to the sums involved, but there are a number of things that event organisers themselves can do to limit their exposure and in turn bring down the cost of cover.

"We try to suggest to all clients that they should try and mitigate as many of the risks as they possibly can themselves," says James. "So if you've got a tour, make sure you allow enough time to travel between event dates and add contingency spare days. There are also clauses within contracts where organisers can try and either share or pass on risk to another party within the contract, whether that's a sponsor, a television company or even a supplier."

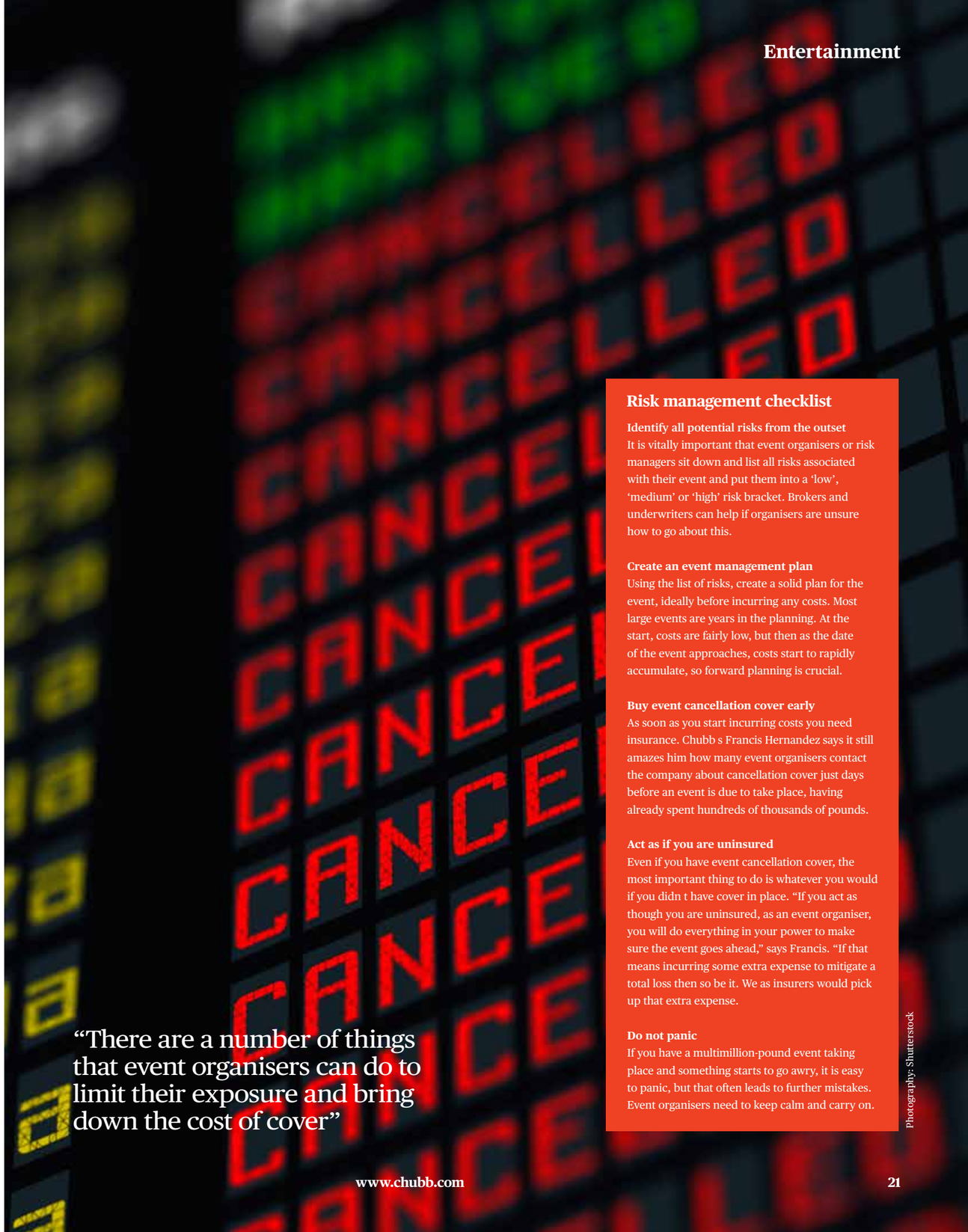
But what do organisers need to consider when weighing up the risks to their event? As a rule of thumb, when deciding whether or not they need cover, organisers should calculate how much they would lose financially if the event did not go ahead. How much would they be able to recoup, could they afford the cost of paying artists and suppliers and refunding ticket sales, or is there a danger that the company could not meet these liabilities and ultimately go bust?

## Know your cover

The other important consideration is what is actually insurable. Organisers cannot insure the projected profit they hope to generate from an event. Insurance policies will only cover their costs and expenses for putting the event on, or the total gross revenue for the event, which includes their income and hopefully their profit.

Of course, there will always be circumstances that neither the organiser nor insurer/broker could have predicted. That is why, when it comes to offering event cancellation cover, providers are deliberately so broad minded, according to James. "There probably are some uninsurable risks, but, at a price, pretty much everything is coverable," he concludes. ■

**Get in touch**
For information on how Chubb supports event organisers to mitigate risks, contact Francis Hernandez, Entertainment Manager for Europe at fhernandez@chubb.com




### Risk management checklist

**Identify all potential risks from the outset**
It is vitally important that event organisers or risk managers sit down and list all risks associated with their event and put them into a 'low', 'medium' or 'high' risk bracket. Brokers and underwriters can help if organisers are unsure how to go about this.

**Create an event management plan**
Using the list of risks, create a solid plan for the event, ideally before incurring any costs. Most large events are years in the planning. At the start, costs are fairly low, but then as the date of the event approaches, costs start to rapidly accumulate, so forward planning is crucial.

**Buy event cancellation cover early**
As soon as you start incurring costs you need insurance. Chubb s Francis Hernandez says it still amazes him how many event organisers contact the company about cancellation cover just days before an event is due to take place, having already spent hundreds of thousands of pounds.

**Act as if you are uninsured**
Even if you have event cancellation cover, the most important thing to do is whatever you would if you didn t have cover in place. "If you act as though you are uninsured, as an event organiser, you will do everything in your power to make sure the event goes ahead," says Francis. "If that means incurring some extra expense to mitigate a total loss then so be it. We as insurers would pick up that extra expense.

**Do not panic**
If you have a multimillion-pound event taking place and something starts to go awry, it is easy to panic, but that often leads to further mistakes. Event organisers need to keep calm and carry on.

Photography: Shutterstock

# Whisky galore

## Thieves are targeting cargo shipments with zeal, and food and drink are top of their lists

The number of cargo crimes skyrocketed in 2016 across the Europe, Eurasia and Africa region, increasing by 72% according to data collected by the Transport Asset Protection Association (TAPA) from 34 countries. The UK saw an even more dramatic spike of 223%.

Food and drink topped the list of product categories for thefts, accounting for 10.6% of the total. In one incident, whisky and wine worth €139,712 disappeared from a vehicle in Northamptonshire after offenders cut the curtain side of the truck.

Goods in transit have been a target for thieves since supply chains began, but the problem keeps getting worse, says Phil Skelton, Chubb s Head of Transportation Risk Management for Overseas General Insurance. “A lot of it is down to the ease of stealing from trucks. There’s very little protection and they’re often parked overnight in lay-bys.

One new, albeit fairly rare, technique used by criminals has been labelled ‘Fast and Furious’. Phil explains: “An SUV comes up behind a moving truck, someone then climbs out and opens the truck doors, passing goods back to the SUV or throwing them out for someone else to pick up. Because the cars get so close to the truck, the driver can t see what’s happening.

A more common approach is deception theft, where the criminal poses as an official at a depot, asking the driver to load their haul into another truck. This is where due diligence can help. “If shippers are using logistics companies, we ask what level of theft awareness training their drivers have.

Phil also advises shippers to include security protocols within their contracts with third parties – for example, stipulations that trucks must be alarmed and have immobilisers, and drivers must have a full vetting record. ■

*For information on Chubb s security assessment services, contact phil.skelton@chubb.com*

Photography: Getty

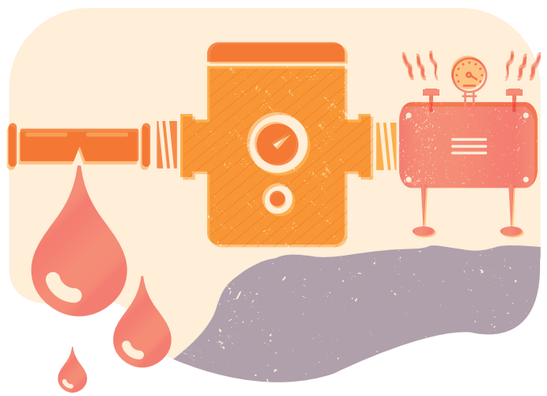
# Plugging a cash leak

A Local Education Authority (LEA) had to shell out £1 million after an oil leak from one of its buildings contaminated a small village. If it had taken out an environmental liability insurance policy and followed correct record-keeping procedures, its clean-up costs would have been completely covered. In this infographic, we look at what the LEA did to incur its hefty bill and what it should have done to make a successful claim

Illustration: Alex Weaver

## 1 Trouble in the air

The first whiff of trouble emerges in 2011, when shoppers in a small Irish village complain about an odious smell inside a nearby shop. Its managers promptly call the Local Authority's environmental health department to come out and investigate. The shop's bosses decide to temporarily close while the investigation takes place. Investigators discover that the odour is emanating from heating oil, with traces of the substance found in a nearby stream and in danger of migrating even further to a lake used for drinking water by the villagers. More work reveals that the oil leak has come from a heating oil tank located on the site of a building used for education across the road from the supermarket and next to the affected stream. After declaring that the oil beneath the shop poses no fire or health risks, it reopens.



## 2 Problem pipe

The LEA calls in a plumber to investigate the five-year-old heating oil tank. He discovers a hole in the pipe connecting the tank to the boiler. He determines that the pipe has corroded just beneath the ground's surface and fixes the leak.

## 3 The claim

The LEA had a property insurance policy and a public liability policy, which a general insurance company had provided through a national broker. It makes a loss of oil claim against the property policy, to which the insurer gives the thumbs up. The insurer also determines that part of the cover is to clean up any oil damage within the building's boundaries. As such it sanctions the use of equipment to dig a hole in the ground to begin cleaning up the oil leakage.

"The LEA, rocked by the decision and intent on continuing to state their case, has no option in the meantime but to pay for the clean-up themselves"

## 4 Disaster strikes

The Local Authority requires that the clean up of the oil needs to extend beyond the property boundary to protect the stream. However, digging does not last long after the loss adjuster working for the insurer on the public liability claim declares that it could not provide cover. The loss adjuster says that, despite the LEA's claim that the leak had happened only in the last week or so, it was probably a gradual pollution event and may have started well over a year before as corrosion of the pipe started. He also declares that as no member of the public has been harmed by the leak, the public liability claim is null and void. The policy cannot be triggered.


## 5 Picking up the bill

The LEA, rocked by the decision and intent on continuing to state their case, has no option in the meantime but to pay for the clean-up themselves. The work leads to a £1 million bill.

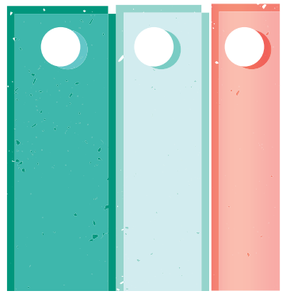
## Lessons from the leak

**What would have saved the LEA from a hefty bill and wrangling with their insurer?**

### Get the policy right

When the LEA purchased its new heating oil tank back in 2006, its best course of action would have been to insure its new acquisition with an environmental liability policy. Even though the building was used for the purposes of education, the LEA (and its broker) should have realised that a heating oil tank is an environmental risk. Such a policy would have covered all the events that resulted from the oil leak in the village. It would have covered the property leakage up to the boundary and the public liability policy extending out from the boundary to the stream. The insurer would have paid out and cleaned up the damage.

"There is not enough knowledge about environmental liability and the limitations of public liability policies when dealing with environmental damage," explains Duncan Spencer, Director of specialist environmental insurance broker EDIA - an Appointed Representative of Property Insurance Initiatives. "However, as more claims are received in this form, we will have more evidence that public liability policies are just not responding."



### Keep records

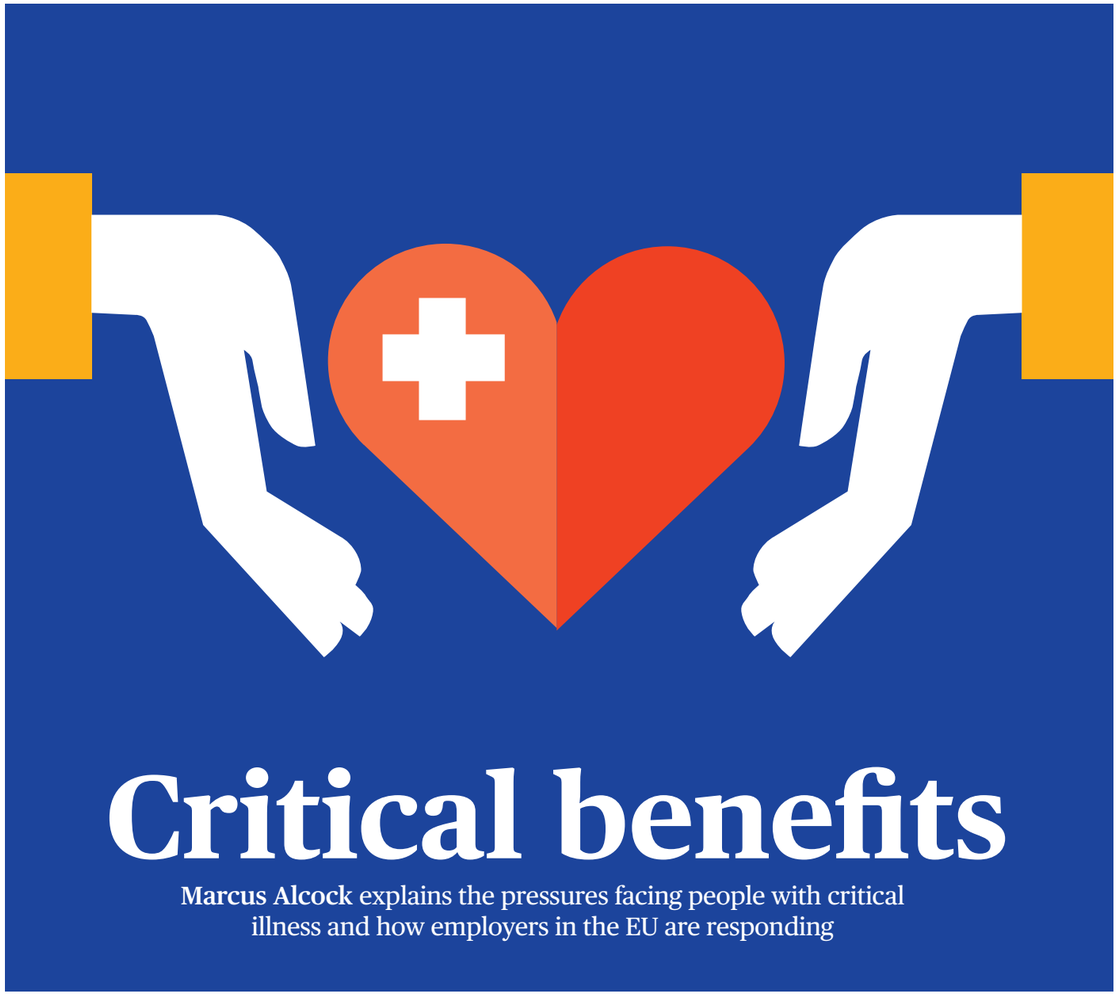
The LEA should have kept better records on how much heating oil it was using from the tank. This was fundamental when it came to proving when exactly the leak occurred. It is not a straightforward calculation, as the amount of oil used naturally changes from month to month and season to season, but there were no clear records showing exactly how much oil was flowing from the tank to the boiler. In the end, the loss adjuster concluded that the LEA, for at least 18 months, had been using above-average amounts of heating oil. This, he believed, was another indicator that the leak had been gradual. The LEA's attempt to prove that it had been a sudden event could not be backed up because it had not kept the necessary records. "If you are an owner of a heating oil tank then closely monitor how much oil is actually being used. If there are any unusual patterns then get it investigated as soon as possible. Up-to-date record-keeping is vital," advises Duncan.

### Talk to each other

The insurer should have had better coordination over the separate property and public liability claims. The insurer believed the property claim had been triggered and sanctioned a clean-up of the ground. However, this was before the public liability loss adjuster had made his call on the claim. His doubts on arriving on site led to the stoppage of the work and a realisation that the property claim should not have paid out. Disastrously, the work that had been carried out - essentially a big hole in the ground - had removed half of the evidence that would have helped investigators calculate how long it had taken the oil to migrate to the stream. "An early and coordinated response is vital when responding to environmental incidents, ensuring that all parties are fully informed and are equipped to respond to the coverage provided under their respective policies," says UKI Environmental Risk Manager Glenn O'Halloran. ■

"The LEA should have realised that a heating oil tank is an environmental risk"

Illustration: Noun Project



# Critical benefits

**Marcus Alcock** explains the pressures facing people with critical illness and how employers in the EU are responding

Despite continuing advances in healthcare and treatment effectiveness, the fact remains that some 50 million people in the EU currently suffer from two or more chronic diseases, such as cancer, heart disease or stroke. In France alone, by 2025, it is estimated that 19.7% of the population will have a serious illness, while the Association of British Insurers tells us that more than one million working people in the UK unexpectedly have to give up work because of injury or illness.

But there is some positive news. Advancements in treatments mean that more people are surviving for longer and managing their illness. For example, data recently published in the *European Heart Journal* suggests that, while cardiovascular disease (CVD) causes more than four million deaths each year in Europe, with more than 1.4 million people dying prematurely (before the age of 75 years), success in preventing and treating the disease has led to large decreases in CVD in a number of countries.

"Cardiovascular disease causes more than four million deaths each year in Europe"

EU countries have done particularly well, with Belgium, Finland, France, Germany, Greece, Hungary, Ireland, Italy and the Netherlands all registering significant decreases in CVD, which includes stroke, over the past decade

### Coping strategies

Despite such encouraging statistics, there can be little doubt that dealing with ►

"With resources in the European public healthcare sector under continuing strain, the support of the private sector is crucial"

**1 in 3**
French people quit or lose their job following a cancer diagnosis

**1.4m**
Europeans die prematurely as a result of cardiovascular disease each year

the emotional and physical effects of critical illness remains a battle. To compound the difficulty, for many people the financial implications can add to the acute stress of coping with a chronic, severe illness. Indeed, the League Against Cancer in France, where one in two men and one in three women get a cancer before the age of 85, has campaigned recently on the issue of the precarious financial position of patients.

The problem is particularly acute for people who work and see their incomes decrease while simultaneously facing escalating outgoings related to their condition. According to 2014 research by the League, one in three French people lose or quit their job following a cancer diagnosis, while three-quarters reduce their daily outgoings on expenses such as food and energy.

With resources in the European public healthcare sector under continuing strain, the support of the private sector, especially where critical illness is concerned, is crucial. Insurance may be particularly relevant to those who do not have substantial savings to help them recover from a period of illness or convalescence, or those who do not have a suitable employee benefits package that would cover them.

Although there is a wide variety of providers operating in the European market at present, and even though cover can vary considerably between carriers, as a rough guide, critical illness insurance will aim to provide a fixed, lump-sum payment following the diagnosis of any illness listed in the policy.

Some policies include, in addition, a per-day benefit for certain treatments, such as dialysis. For individual policies, the benefit payments can be made directly to the insured and can be used for any purpose, such as covering deductibles, medical co-payments, income shortfalls and travel expenses. The cost of such a policy will vary, based on factors such as age, smoking and pre-existing conditions. An insurer may also consider family health history, looking, for instance, at any hereditary issues such as heart disease.

Such cover would appear to offer a significant financial cushion, given that, according to recent research, 60% of people who are professionally active before they have cancer report having lost income. Indeed, in 44% of the cases, these active people lost more than a quarter of their income, potentially putting their property at risk.

In France, where group personal accident insurance accounts for approximately 50% of all accident and health insurance, the government has taken action on this issue. New regulations were introduced last year, requiring all private companies, irrespective of their size or sector of activity, to provide group critical illness schemes for each employee, whatever their status or seniority. The cost can be shared between employer and employee with a minimum 50% of the cost born by the employer.

According to Stephane Baj, Director of Corporate and Affinity, Accident and Health for Europe, Eurasia and Africa, such group cover is likely to become increasingly popular. As companies search for insurers, they will find that some offer services beyond financial help, including access to medical experts who can confirm diagnosis and help formulate a treatment plan, and assessments to predict the risk of contracting illnesses such as diabetes, high-frequency cancers and heart failure.

"For employees," Stephane says, "such cover enables them to manage their health better. For the company, it can also help to improve productivity, better manage absenteeism and contribute to their corporate social responsibility."

## The caring company

Naturally, there are bigger socioeconomic drivers motivating businesses to take an interest in critical illness cover: an increasing need among employees, financial constraints on healthcare systems and the need to attract and retain talent, as well as Europe-wide regulation, which Stephane says "brings more and more needs and duties of care to companies towards their employees. They are interested in solutions that help them to not only meet their duty of care, but also to go beyond this in helping them boost their human capital."

By moving beyond the traditional model of monetary compensation to a model of insurance that embodies prevention as well as treatment, it would appear that the European accident and health market really is doing its best to engage with employers by helping them achieve genuine improved health benefits for their employees. ■

### Get in touch

If you would like to find out how Chubb helps people to prepare for the risk of critical illness and the services is provides if the worst does happen, please get in touch with Stephane Baj at stephane.baj@chubb.com.

# Wake-up call

When the WannaCry virus was unleashed in May, the scale of global vulnerability to ransomware became startlingly apparent, as did the importance of cyber-specific insurance, says **Tony Dowding**

Over 200,000 computers in 150 countries were affected by the indiscriminate WannaCry attack, which led to operations being cancelled, factories being closed and work disrupted at companies big and small. But the virus is just one of millions of ransomware attacks each year, and the impact goes far beyond the cost of ransom payments.

In its latest *Internet Security Threat Report*, Symantec Corporation found that ransomware was one of the most significant threats facing individuals and organisations in 2016 due to its prevalence and destructiveness. For Chubb, it is the fastest growing type of cyber claim and makes up the lion's share of reported incidents.

The ransoms are generally small amounts, although they are growing - the average ransom amount was $1,077 (€920) in 2016, compared with $294 (€251) in 2015, according to the Symantec report. But, as Kyle Bryant, Regional Cyber Risk Manager for Europe at Chubb, explains, the real damage is caused when a ransomware attack hits a critical system, or spreads into the computer network. And for systems that are open and flat, such as in a hospital, it can spread very quickly to the server and across the entire organisation, as the WannaCry virus showed.

"One of the first things that happens is that you are locked out of your systems," explains Kyle. "Then it is a question of whether to pay the ransom. This will often be made to a random email address or Bitcoin account. But you are not negotiating with a criminal enterprise in order to obtain delivery of an item on your terms. It is an anonymous transaction where you are not even guaranteed that you will receive an encryption key."

Indeed, according to research carried out by the Norton Cyber Security Insight team, 34% of victims pay the ransom, but only 47% of those report getting their files back. If a victim does not pay, the next step is to restore from backup. "Running regular backups will limit your loss," says Kyle. The process may involve running two systems simultaneously, or just backing up every hour, or every day. Certainly, the days of running a backup once a week or once a month should be over."

Training is a vital element of ransomware risk mitigation. Glyn Thoms, Executive Director Cyber & TMT at Willis Towers Watson, explains: "From our claims data, we see that around two-thirds of incidents are a result of acts of employees, whether malicious or negligent. So you need training and awareness around cyber security and an educated workforce."

Kyle agrees that training is part of good cyber hygiene, but also emphasises the importance of preparation. "Humans are the vulnerability and we know that training works. But you will only be able to improve things a little. For companies that have thousands of employees, it is a significant vulnerability. At that point, they need to focus on their ability to respond."

> "One of the first things that happens is that you are locked out of your systems"

In response to the WannaCry virus, some companies have attempted to use kidnap, ransom and extortion policies to claim for losses. Glyn says that cyber extortion cover has tended to be added into kidnap and ransom (K&R) policies over the years and he explains that, from a client point of view, it is attractive as it is often included for free, and generally there are very low, or even zero, retentions on a K&R policy.

But he says this poses challenges for the K&R insurance market in terms of claims that were not underwritten and priced for, so the market has started to harden and insurers have less of an appetite for that cover. K&R policies can also leave companies under-insured when an incident occurs.

"Ransomware attacks can have a cascade effect, often leading to network interruption, extortion payments, potential privacy and regulatory issues, and a specific cyber policy is able to pick up all of those, whereas a K&R policy is more targeted at the extortion payments," says Glyn.

There are significant problems with using K&R for cyber extortion, according to Kyle. "Does your insurance policy (whether kidnap and ransom, crime or cyber) cover data restoration or reconstitution? Will recoding be required for critical systems that will prolong the business interruption? These losses will not be covered in traditional crime or kidnap and ransom policies," he explains.

## Calling in backup

Another consideration is the third-party support that might be required to deal with an attack. Ransomware can sometimes be 'time-bombed' (programmed to trigger after a delay) and it can get into the backup, so companies will need to perform significant scans before restoring systems, which may require a dedicated IT expert or IT forensics team.

In addition, PR and crisis management costs can be incurred, as well as legal costs from follow-on liability claims relating to contracts, suppliers, stakeholders and customers. Bigger companies also face regulatory challenges.

Cyber insurance policies can help cover these costs and ensure that companies do not have to pay the ransom. "We do not, as an insurer, want to promote the success of criminal enterprises, so we would much prefer it if companies can recover without paying the ransom," explains Kyle. "Cyber policies are designed to achieve this by bringing in expertise where it is required in the critical time period for the client, so that they have the best information to make the right decision."

Glyn agrees that preparation and appropriate cover are key to mitigating this kind of risk: "Having a response and recovery plan in place prior to an incident, and having it tested effectively and regularly, will be critical to ensuring speed of recovery and therefore mitigating the longer term financial and reputational impact. And cyber insurance can be there to help, covering the cost of the services to enable a company to recover in the first instance, and also picking up the longer term costs and liabilities and potential regulatory issues that may come into play."

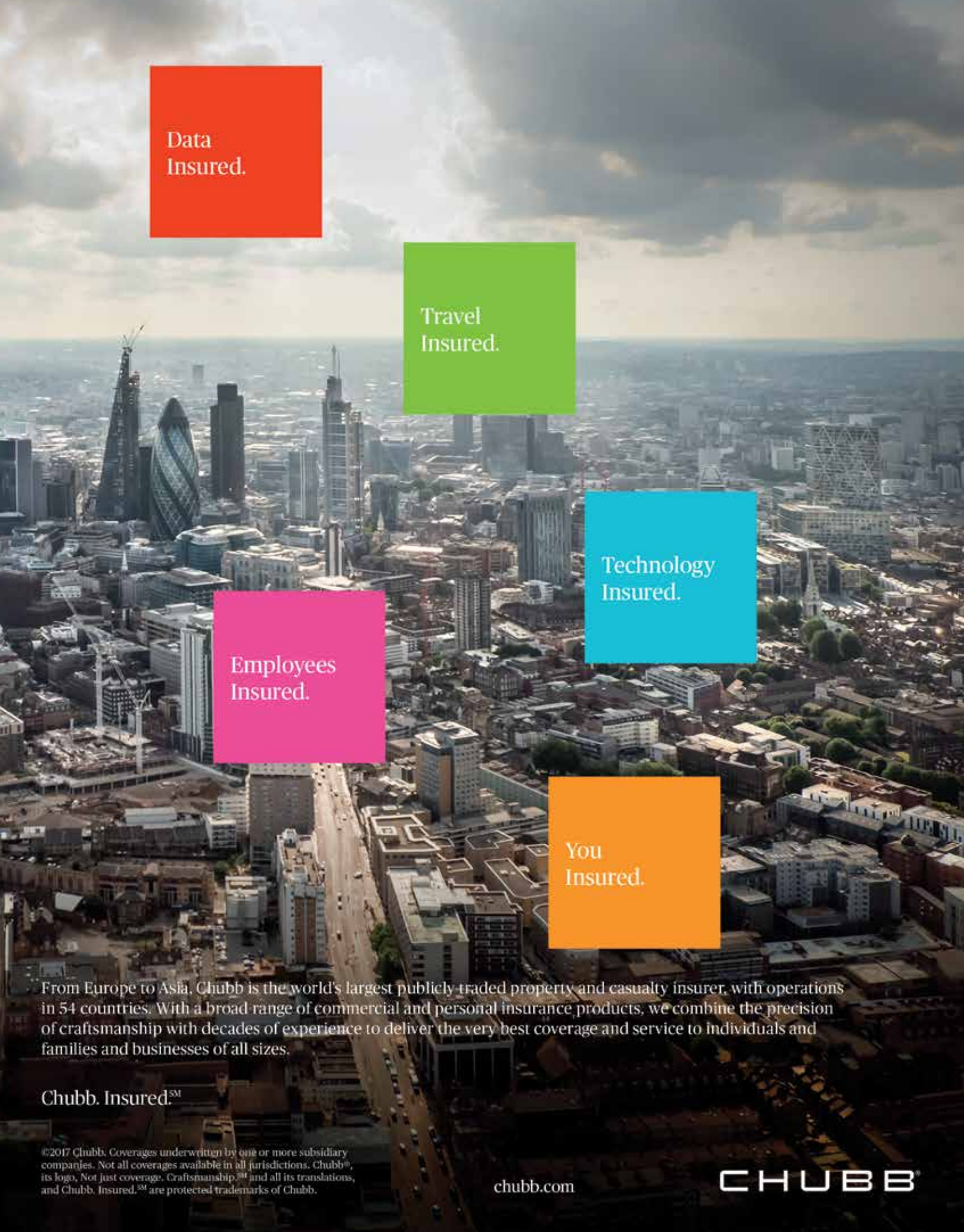
The WannaCry virus came as a shock to the world, but hopefully the wake-up call it has provided will mean other companies are prepared for the next attack. ■

Photography: Getty Images

### Top tips for protecting against ransomware attacks

- New ransomware variants appear on a regular basis. Always keep your security software up to date.
- Keep your operating system and other software updated too. Software updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by ransomware attackers.
- Email is one of the main infection methods. Delete any suspicious-looking emails you receive, especially if they contain links or attachments.
- Be extremely wary of any Microsoft Office email attachment that advises you to enable macros to view its content.
- Backing up important data is the single most effective way of combating ransomware infection. Attackers have leverage over their victims by encrypting valuable files and leaving them inaccessible.
- Using cloud services could help mitigate ransomware infection, since many retain previous versions of files, allowing you to 'roll back' to the unencrypted form.

*Source: Symantec Corporation Internet Security Threat Report*




From Europe to Asia, Chubb is the world's largest publicly traded property and casualty insurer, with operations in 54 countries. With a broad range of commercial and personal insurance products, we combine the precision of craftsmanship with decades of experience to deliver the very best coverage and service to individuals and families and businesses of all sizes.

Chubb. Insured.℠



chubb.com

CHUBB®