CHUBB

2018 Issue 1

Progress

Trial and error

Tailored treatments are changing pharma risk

Crown jewels
Mistakes to avoid when storing valuable items

Whistle while you work
Is your whistleblowing policy up to scratch?

Spectator esports
With computer game tournaments worth millions, what are the risks?

Welcome

Rapid technological transformation and scientific breakthroughs touch almost every aspect of our lives, whether at work or home. As a result, the landscape of risk and opportunity is shifting constantly and at increasing speed. Risk managers are on the front line in terms of deciding whether these changes represent a threat or an opportunity and this can be a challenge sometimes.

In this edition of *Progress* magazine we look at the risks around the remarkable area of personalised medicine (p10), which targets disease prevention and treatment for individuals. We also consider the growth of the industrial internet of things (p17) and what it means for the future both in terms of the efficiencies this offers and also the potential for trouble. Being better connected brings clear advantages to business but it also opens up new dangers that need to be recognised, understood and mitigated or transferred. As the article explains, the exposures associated with the IoT are multi-faceted and not always obvious. Technology is also transforming the world of sport as computer game tournaments move into the big league of spectator entertainment. Of course, not all risks are new, our article on protecting your collectibles (p6) is a must-read for anyone with a home full of valuables. Natural disasters are perhaps the oldest risk of them all and the dangers they pose have not diminished over time. Also in this issue (p14), we look at the role of insurance for business in the immediate aftermath of a major incident, when more than financial security is required. We hope you enjoy reading these and all the other articles in *Progress*.

David Furby
Regional President, Europe and
Senior Vice President, Chubb Group

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 SE registered in England & Wales number SE000116 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/

IMPORTANT NOTICE: In order to prepare for the UK's exit from the European Union, Chubb is making certain changes. To stay up to date with our Brexit preparations and for more information about what it means for you, refer to our website at chubb.com/Brexit

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

Cover illustration: Alex Weaver

6

14

22

The road ahead

In an ever-changing and uncertain geopolitical landscape, risk managers should rely on insurers that build capabilities by simplifying current challenges and investing in future needs says, **Suresh Krishnan,** Head of Global Accounts for Europe

When we think of the past, we often recall with fondness how much simpler things were. Before technology was a disrupting force, when there was a modicum of consensus in politics, and when climate change was not in the vernacular. Whether or not we live in less stable times today is debatable, but the sense of geopolitical instability is undoubtedly stronger than it has been. This represents an opportunity for risk managers to show leadership and foresight when navigating an uncertain future.

So what should risk managers demand from their multinational insurers? Multinational insurers must demonstrate that they have the capabilities to help risk managers show leadership and foresight when navigating an uncertain future. The 'must-have' capabilities begin with People, with skills that can underwrite and manage cross-border uncertainties; then Presence, connected by an international network; Solutions, having the right specialist products available globally; Technology that simplifies a complex world; and, most importantly, unparalleled Service, the true differentiator.

First, insurers must share what they know through thought leadership, both in terms of subject matter and product expertise. Staying ahead of evolving risks is challenging, and research such as Chubb's recent report *Bridging the Cyber-Risk Gap* provides time-saving lessons (see page 22). A key conclusion of the report is that many companies have not reached a consensus on whether cyber security is the responsibility of IT or risk management. In other words, whether priority should be given to preventing or treating cyber attacks. The implication is that both teams need to work together better to manage threats and define clear lines of responsibility. Those who fail to do so will leave vulnerabilities that can be exploited.

Second, multinational businesses are particularly sensitive to some of the risks characteristic of our uncertain world. This is another area where insurers can help. Insurers should demonstrate they can service, across national borders, core multinational solutions – property, casualty, directors & officers liability – and specialty multinational solutions, such as multinational business travel accident, cyber risk, environmental risk, terrorism risk and surety. These are integral to managing some of the headline risks of today. Servicing also includes not just having a location, but a network that connects multiple local offices, seamless and transparent cash movement, local claims capabilities, manuscripted tailoring of local policies, and a repository of local knowledge, from custom and practice in local countries to up-to-date compliance information. Additionally, when clients want certainty in a multinational programme, it often means they want a claim to be paid locally. Having owned local offices in countries where clients reside, with an international network connecting people on the ground and local expertise in a specific line of business to handle claims, is imperative to multinational programme success.

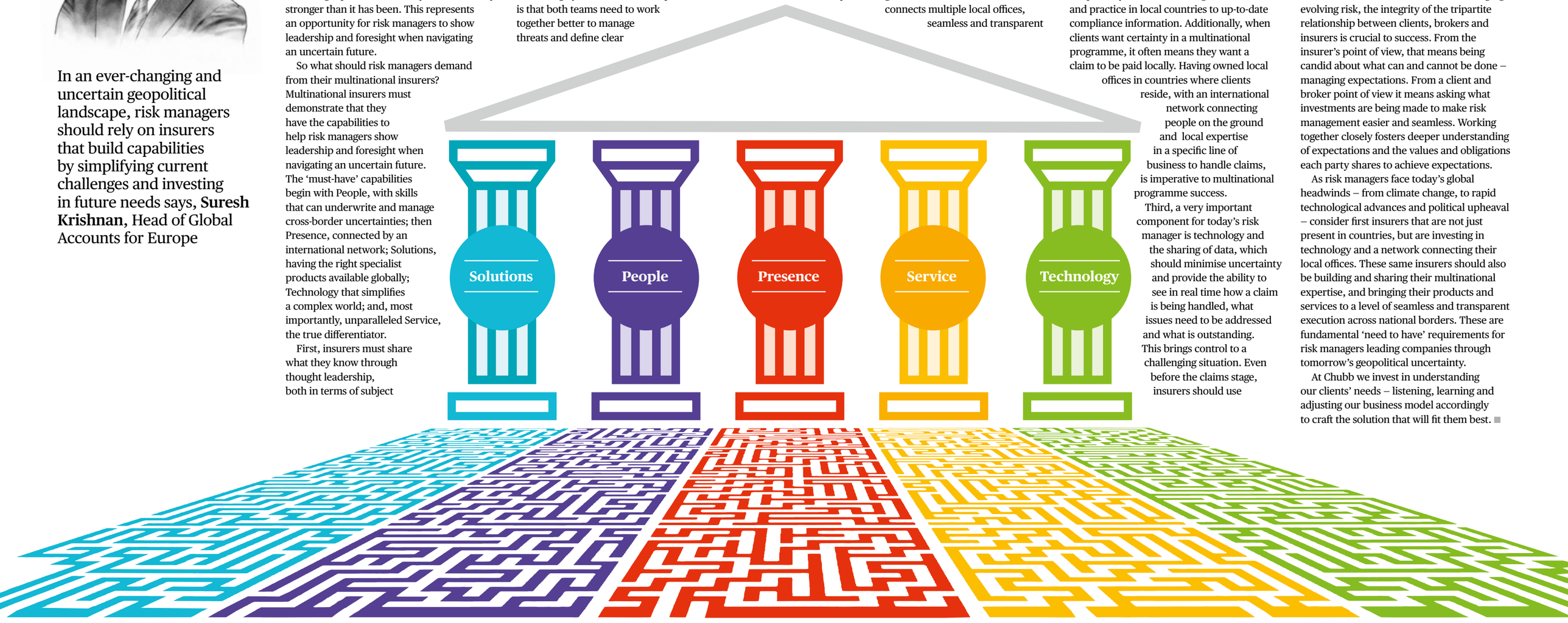
> "The 'must-have' capabilities begin with People, with skills that can underwrite and manage cross-border uncertainties"

Third, a very important component for today's risk manager is technology and the sharing of data, which should minimise uncertainty and provide the ability to see in real time how a claim is being handled, what issues need to be addressed and what is outstanding. This brings control to a challenging situation. Even before the claims stage, insurers should use technology to profile clients' risk and share this with clients. Every client is unique, even within an industry class, so insurers must ask for and use client data in order to ensure the viability of a multinational insurance programme is assessed properly. Clients sharing data with insurers should expect underwriting and claims scenario planning based on the data gathered by insurers, especially comparing peers in similar industry classes. Clients should ask for this as part of building a longer-term relationship with their insurer.

Fourth, and implicit in all of this, but equally important, is transparency and communication. When it comes to managing evolving risk, the integrity of the tripartite relationship between clients, brokers and insurers is crucial to success. From the insurer's point of view, that means being candid about what can and cannot be done – managing expectations. From a client and broker point of view it means asking what investments are being made to make risk management easier and seamless. Working together closely fosters deeper understanding of expectations and the values and obligations each party shares to achieve expectations.

As risk managers face today's global headwinds – from climate change, to rapid technological advances and political upheaval – consider first insurers that are not just present in countries, but are investing in technology and a network connecting their local offices. These same insurers should also be building and sharing their multinational expertise, and bringing their products and services to a level of seamless and transparent execution across national borders. These are fundamental 'need to have' requirements for risk managers leading companies through tomorrow's geopolitical uncertainty.

At Chubb we invest in understanding our clients' needs – listening, learning and adjusting our business model accordingly to craft the solution that will fit them best. ■



The fine art of insurance

Protecting the value of your prized collections and making sure they are insured takes long-term thinking, says **Andrew Pring**

When Leonardo da Vinci's *Salvator Mundi* sold in New York in November for $450 million (€382 million), after a frenzied 19-minute bidding war, it became the most expensive painting of all time. What made the bid even more astonishing was that the 16th century masterpiece had been valued beforehand at $100 million.

Welcome to the volatile world of trophy art, where uber-wealth in pursuit of rarity, popularity and desirability can drive prices to dizzying heights. Other record-breaking collector's pieces over the past few years have included Picasso's *Nude, Green Leaves* and *Bust* ($106 million, 2010), the Wittelsbach diamond ($23 million, 2015), Michael Schumacher's Ferrari ($7 million, 2017), a piece of 18th century furniture called The Badminton Cabinet ($36 million, 2004) and even the dress Marilyn Monroe wore to sing 'Happy Birthday, Mr President' to John F Kennedy ($5 million, 2016).

But once you have jumped the hurdle of securing the object of your desire, it is important to know how to protect its value. From a risk-transfer perspective, the best way to do this with any high-net-worth collection is to have each piece independently valued by an expert. That way, any insurance claim can be handled efficiently.

Once independent valuations have been established, owners should create a detailed inventory listing each piece with supporting documentation. The rule of thumb is that you cannot document your collection too much. Original sales receipts, certificates of authenticity, valuations and evidence of regular maintenance and servicing, along with photographs of each item should all be filed and stored securely.

> "An appraisal will make sure sums insured are agreed up front so the insurer and the client know that a claim will be settled at the sum shown on the schedule – nothing more or less"

Home appraisals carried out by insurance companies help make sure all of this is in order. Brian Verney, Senior Risk Consultant, Europe - Personal Risk Services at Chubb, explains: "An appraisal will make sure sums insured are agreed up front so the insurer and the client know that a claim will be settled at the sum shown on the schedule - nothing more or less."

But appraisals also identify risks to a collection and propose preventative measures, which, as Brian is aware, can be a sensitive point. "The balance of storing an item securely and in the best conditions can be a personal choice for the client," he says, "but a common sense approach is generally prudent. Balancing the want to enjoy an item but still protecting its intrinsic value is important."

One common problem identified during appraisals is poor fire prevention measures. "We recently visited a client who had only two smoke detectors for the whole property, both located in the swimming pool complex with no detection equipment covering the main residence. This would be a serious concern for most homeowners, let alone those with valuable art collections," explains Brian. As a precaution, Brian advised that the client fit additional smoke detectors in the main property. Both the client and broker were sceptical about the advice and despite the modest outlay of approximately £2,000, declined to accept the requirement for additional fire detection. However, the potential risk was there for all to see and the appraisers and underwriters stood firm on their position. After more than a month's negotiation, the client eventually agreed to have the work done. Three months later, the property suffered a fire when the sun's rays were reflected by a mirror onto clothing in one of the bedrooms. Almost immediately, ▶

the new fire detectors were activated and the homeowner was able to deal with the small fire himself.

Home safe

Losses come in all shapes and forms, with fire presenting one of the most obvious risks to any owner's artworks, but negligent storage and display may also prove extremely harmful. So too can human error, as the American businessman Steve Wynn discovered in 2006, when an accidental blow from his elbow damaged a Picasso he had reportedly just agreed to sell to a fellow tycoon for $139 million, delaying *La Rêve*'s purchase until insurance-backed repair was effected.

Other forms of potential damage can be less immediately obvious. Chubb recently appraised a fine art collection for a client using thermal imaging technology and uncovered a potential risk that was invisible to the eye.

Two particularly unique items, a Francis Bacon and wooden installation, were hanging on either side of what appeared to be a solid wall. However, the thermal camera detected a floor to ceiling heating pipe inside the wall displaying a range of different temperatures.

> "Art values can often go up at a far greater rate than inflation, particularly in periods like this, with so much cheap money flowing into the salesrooms"

The risk of warping or water damage was significant enough to persuade the client to relocate his valuable artworks to a more suitable location.

Similarly, an acrylic painting hung in a chateau in the South of France, where there is stronger light and higher humidity, would need to be stored and cared for in a different way from a painting in, for example, cooler, wetter Scotland. And equally, fine wine, artworks, classic cars, cameras and watches all have unique transportation, maintenance, storage and display needs that vary region-to-region.

Climate-controlled units will sometimes be necessary to avert harms caused by UV exposure, high temperatures and humidity. Collectors of stamps, comics, coins and musical instruments must also adopt similar safeguarding measures. And all these considerations should be backed up, of course, with high security.

Preservation techniques have moved on substantially in recent times. Brian says: "Technology is now being used more frequently to achieve uniform storage conditions for anything from a classic Ferrari to a 100-year-old teddy bear!"

Keep your eye on the prize

Collectors should also stay on top of the fluctuating value of their prized possessions to ensure they are appropriately covered. Insurance companies are able to recommend independent experts for this purpose.

Stephen Meadowcroft is a Director of Valuation Services at international art advisers Gurr Johns, which evaluates annually more than €8 billion worth of highly desirable objects. With 40 years of experience in the business, he is used to the market's febrile excitements - the downs as well as the ups, as prices can sometimes fall disappointingly short of expectations. As to the occasional expert-defying leap in value, "It happens - in an auction, it just takes two people," is his seasoned view.

"Prices have been boosted over the past few years, not least by cheap money and a new wave of collectors from China, Russia and India" he explains. "And a lot of the new money goes into top-end modern and contemporary art, as well as other 'trophy' works of art."

It's not just art that's going up, says Stephen. "Cars are doing amazingly well too, from Jaguar E-types to rare Ferraris, and even more recent supercars like the McLaren F1. Jewellery is also increasing in value - up 8% year-on-year - and watches can fetch very high prices. In October in New York, Paul Newman's Rolex Daytona made almost $18 million - a staggering sum."

An expert in this rarefied field, Stephen is regularly called in by insurers to assess the value of a client's art collection, as well as other high-value items they may possess.

With values rising regularly, and often vertiginously, the risk of insured possessions becoming under-insured if a claim occurs a few years after the initial valuation is very real.

"Art values can often go up at a far greater rate than inflation," says Stephen, "particularly in periods like this, with so much cheap money flowing into the salerooms. To keep fully abreast of the market, we've developed a set of indices over the past decade that constantly tracks price movements in hundreds of categories, making sure that we always have an up-to-date knowledge of current values."

Reassessment of insurance policies is advisable for reasons beyond fluctuating values. In a recent case that Chubb came across, the jewellery sum insured was originally set at £1.2 million (€1.3 million), but various additional items had subsequently been bought by the owner. Following a full revaluation, the sum insured was revised to £13 million. One ring alone was worth £2 million.

However, you can be over-insured too, so taking a proactive and regular look at existing policies is important. The environment where items are stored can also change, as can the technologies for looking after them. So whether it is the price of your collections or how you keep them, revaluating the situation regularly is key to protecting their value, and the insurance industry is here to help. ■

Top three lessons for collectors

1. Document your valuables - this cannot be stressed enough. A comprehensive paper trail will facilitate any claims.
2. Ask for an appraisal - not just of the value of items, but also how and where you keep them.
3. Re evaluate constantly - stay on top of price fluctuations so that you have the appropriate level of cover. The environment where you store your prized possessions can also change and new technologies emerge regularly that can help preserve them.

Photography: Alamy, Getty Imgaes, iStock







Illustration: Alex Weaver

Healthcare, tailored to you

Advances in medical research mean treatments can be personalised to a patient's circumstances in ways previously only seen in science fiction. **Nick Renaud-Komiya** examines the potential risks for those companies creating this new generation of medicine

More often than not, the medical diagnoses and treatments we receive are given on the basis of trial and error. But that is changing, thanks to the emergence of personalised healthcare made possible through advances in genome sequencing.

After two decades of unravelling our genetic code, it has now become possible to examine information about an individual's DNA that was previously difficult to access. Properly harnessed, this data can provide us with clues as to the best way to treat and even prevent particular illnesses.

Claire Wilkinson, London Senior Life Science Underwriter at Chubb, explains: "There is a big trend towards personalised healthcare for disease prevention and personalised medicines for treatment of diseases. These drugs are going to be more targeted, producing fewer side effects for the patient. For example, chemotherapy currently affects healthy as well as cancerous cells. If treatment can be targeted on cancer cells only then higher doses can be given resulting in better outcomes for the patient and, while the side effects won't be gone altogether, there will be fewer of them."

Across Europe governments, researchers and the healthcare industry have been exploring the practical ways in which this new, data-rich approach to developing treatments can be harnessed to improve public health outcomes.

> "After two decades of unravelling our genetic code, it has now become possible to examine information about an individual's DNA"

These advances are not just confined to pharmaceuticals, there are huge advances in medical device development and healthcare information technology. For example, the use of virtual reality. Claire states "Many university hospitals are using virtual reality in surgery. A surgeon may practice a hip replacement operation in the virtual space before commencing surgery on the patient. Recently surgeons used virtual reality to assist in the successful separation of conjoined twins by being able to use the MRI and CT scan images to form a virtual model that, using virtual headsets, meant they could look inside the anatomy of the twins before and during surgery."

Personalised medicine is still at a relatively early stage across Europe when compared ▸

"Those developing personalised treatments typically find it much harder to amass that much trial data"

with the United States. According to Thomas Sproho, Chubb's Life Science Regional Manager Continental Europe, that's partly because the US has regulations better adapted to this new kind of treatment. However, activity in personalised medicine is increasing. For example, the French government is investing €670 million by 2020 in a genomics programme to improve diagnosis and prevention of disease, with the health minister describing personalised medicine as a "revolution". And a cross-governmental initiative, the Genomic Medicine 2025 Plan, aims to position France as a leading exporter of expertise in the field by the middle of the next decade.

Thomas explains: "France is a really innovative market in terms of research and development. They have a strong network of biotech firms, in what we call incubators - a group of companies pitching together in a big circle to advance common best practice and targets, and to find common solutions to problems."

Elsewhere, the UK government's Department for Health and Social Care states that it is at an "advanced stage" of a plan to integrate genomic and personalised medicine into the day-to-day delivery of care through its 100,000 Genomes project. Meanwhile, European Union member state policymakers and research funders have formed the International Consortium for Personalised Medicine. The group, which is partly funded from the EU's Horizon 2020 Programme, aims to establish Europe as a global leader in personalised medicine research and, in its own words, "pave the way for personalised medicine approaches for citizens".

But while the benefits for future patients are easy to picture - more targeted treatments with higher chances of success and lower costs for healthcare payers in the long term - it raises key issues for the companies trying to develop and trial this new generation of treatments.

Regulatory drag

Unlike more conventional pharmaceutical research and development - which can require a new drug be tested on many thousands of patients to determine its safety and efficacy - those developing personalised treatments typically find it much harder to amass that much trial data. This is particularly problematic if they can only test these drugs on a comparatively small eligible patient group.

Claire, herself a former clinical research professional, explains: "The issue you have with any shift in the life sciences sector is that the current trial process is slow. It takes years to develop treatments and regulations don't keep up. The ability to get the right data from trials to satisfy regulators is difficult. You have to conduct the trial in thousands of patients to make the data robust. You then submit all the data to the regulator."

She adds: "With personalised medicines, you might not be able to get the amount of data required by the regulations. So, the regulations need to be modified. A start-up, with maybe four people and a molecule, has to conduct trials in the same way as a large pharmaceutical company."

This clearly has knock-on effects on the speed with which innovative personalised can be brought to market. However, Claire hopes that as the market in personalised treatments grows, regulatory bodies will be persuaded to streamline trial requirements.

There are also risks where personalised therapies and medical devices are bought online without the oversight or advice of a medical expert. Peter Rudd-Clarke, legal director at professional services firm RPC, warns: "There is a trend towards some people purchasing medical intervention over the internet, which takes qualified medical intermediaries out of the equation. As a manufacturer there could be an increased risk if you do not provide your product via a qualified, experienced medical professional.

"Manufacturers have to try to predict how their treatment may be used. If someone buys your product and uses it for an alternative but foreseeable purpose, you run the risk that a court says it was predictable that it could be used in a way that was not intended and that you didn't properly warn against misusing the product."

"Depending on the product, it may be less risky for manufacturers to sell only to a qualified medical intermediary. So, if a manufacturer is providing equipment and training to a doctor, then the manufacturer is entitled to argue that it provided the information to the doctor. The doctor then uses their clinical judgement in deciding what to do next. That's a good line of defence for a manufacturer and for their insurers."

However, incoming EU regulations should offer diligent life sciences companies some added protection against product liability litigation. The Medical Devices Regulation, due to come into full force in 2020, will require manufacturers to collect more data about the safe performance of their devices before they reach the market. Once on the market, product-makers will then have greater responsibility to track how their products perform.

Peter suggests that while this might be more onerous and costly for manufacturers, it is likely to reduce their product liability risk: "On a practical level it should mean that during the manufacturing process any concerns about the device will be picked up; for riskier products, the new regulations provide that other bodies can demand information."

The cyber risk

The increasing use of sensitive patient data brings a risk of either being a victim of cyber crime or of breaking cyber rules. The complexity of navigating different national rules governing the use of such patient information means that life sciences companies may, even inadvertently, find themselves on the wrong side of the law.

Last summer, DeepMind, Google's artificial intelligence arm, was in hot water after the UK authorities found that a London-based NHS organisation had broken data protection laws when it gave the firm access to 1.6 million British patients' medical records.

Thomas believes that cyber-related exposure is slowly on the increase and life science companies aren't necessarily aware of the risks: "For me, cyber is an increasing form of exposure. I don't know if life science companies are aware of the risks or if they consider that the exposure for them is limited because the sector is so highly regulated.

"Personal data needs to be stored in a specific data centre, which will have an agreement for processing medical data."

Another risk, suggests Claire, is that personalised medicine may rely on greater use of software either integrated into a medical device or to support planning / set up / analysis of a personalised therapy. Examples include wearable technology; a medical 3D printing company using CT scan data; or an algorithm for a cancer patient undergoing a targeted therapy for their subtype of disease.

Companies can help mitigate these risks by tailoring insurance cover so that it includes not just the medical product, but also the specialised computer equipment and software used to support the product or the diagnostic process.

Ultimately, the new possibilities for the healthcare sector brought about by advances in our understanding of each person's genetic make-up present boundless opportunities to improve our care. As long as those leading the charge are aware of the potential stumbling blocks and tailor their approach to the risks accordingly, we can look forward to a future where healthcare wraps around the individual's needs much more closely. ■

Reducing the risks: top tips

1. Life sciences firms should be extremely careful about engaging directly with patients and the end user of personalised products. Filtering any communication through qualified medical intermediaries is essential to minimise the risk of litigation.
2. Manufacturers of next-generation medical products and devices can reduce their product liability risk by preparing early for new EU Medical Devices Regulation, due to come into force by 2020.
3. Companies sponsoring or conducting trials of new personalised therapies can benefit from insurance cover better tailored to mitigating against the cyber risks stemming from the use of patients' genetic data.

Get in touch

For information on Chubb's life sciences services, contact Scott McFarlane at SMcFarlane@chubb.com, UKI Regional Life Science Manager, or Thomas Sproho at thomas.sproho@chubb.com

Force of nature

If there is one category of risk that cannot be prevented it is weather related catastrophes. When disaster strikes, it is important to have the right insurer by your side, as **Simon Creasey** discovers

On 29 January this year, the water level of the River Seine peaked at 5.8m, more than 4m higher than normal. The river swelled following the heaviest rainfalls recorded in half a century and wreaked havoc across the French capital, with nearly 1,500 people evacuated from their homes. Even part of the Louvre Museum was forced to close as the flood waters threatened to consume it.

Thankfully, catastrophic events such as this are still relatively rare, but over the past few years there seems to have been a spate of devastating natural disasters around the world, ranging from monsoons, hurricanes, earthquakes, mudslides and tsunamis through to wildfires and flooding in mainland Europe.

It is difficult to establish with any certainty if catastrophic events are occurring with greater regularity. John Latter, UK and Ireland Claims Director at Chubb, says that if you track 'CAT' events back to the early 2000s there have been benign years and there have been years when events occurred more frequently.

"What 2017 showed was a combination of frequency and severity of events," says John. "We experienced a higher than normal level of catastrophic events some of which were very severe. Severe both in terms of impact from a humanitarian perspective and also from a financial perspective. When you look at 2017 it was a very active year for CATs, and when you add the impact of all of these events together, it was possibly the most financially significant year ever."

The first half of 2018 saw fewer claims for natural catastrophes than 2017. But Europe was reminded of the danger of extreme weather by the heatwave that exacerbated wildfires.

In addition to domestic risks resulting from catastrophic events, companies also need to consider risks to their overseas supply chains. This was a major issue for many companies in western Europe following the Japanese tsunami in 2011.

"People tend to think just about what's in front of their door, but you have to realise in a world that is so interconnected, and where supply chains are so intertwined, you can't just look at this from a domestic point of view," says Marc Scheidegger, Claims Director Continental Europe at Chubb.

Some of the financial burden can be offset by insurance. So when a catastrophic event occurs, how are insurance claims assessed and what sort of support can insurers provide?

Regardless of where in the world an incident occurs, John says speed is of the essence and it is vitally important that policyholders make contact with their insurer as soon as physically possible following the event.

> "In a world where supply chains are so intertwined, you can't just look at CAT events from a domestic point of view"

"That early notification is critical," he explains. "It's only when people are aware you have suffered a loss that they can start to swing into action. You have to remember that with some incidents the damaged areas might be inaccessible. So, for instance, the policyholder may know that in all likelihood their factory is damaged because it's in the middle of a flooded area, but there is no way they can gain access aside from using technology, such as drones, which insurers can deploy. Through the use of this technology we can start to determine whether we can gain access, and ask: can we mitigate the loss, what resources do we need to deploy and what's the availability of those resources? We can then set the claim on the correct path towards remediation."

What to ask of your insurer

A good insurance company will also ensure that their policyholders know the correct protocols to follow when a catastrophic event occurs, and they will understand the business of their client, the exposures the client faces and the "intricacies of their unique insurance programme," according to Rob Kleinveld, Executive General Adjuster and Vice President Global Markets at loss adjusters Crawford & Company.

"The closeness of the relationship is central to ensuring that it is precisely aligned to that exposure profile and ensures that in the event of a loss the potential for any surprises is greatly reduced," says Rob. "That relationship spans the broker and the claims adjuster to enable the most efficient response in the event of a loss. Having a preferred or nominated adjuster, who fully understands the insured's business and programme, means that they can respond quickly and sometimes creatively given the unique demands of the claim, to ensure a professional claims response."

It's a view shared by John, who says the key thing insurers need to do during these difficult periods is to support the policyholder and help them get their business through ▶

the crisis. "We need to look at how we support their business. Is there a way of managing their business from another location that isn't under water in the event of a flood?" says John.

"It's looking at what is the immediate need of the policyholder. There are some immediate steps around supporting the policyholder through the initial stages of the crisis and then, longer term, it's all about how do we reinstate the business to the position they were in before the loss and what's the most credible, efficient and quickest way of doing that?"

Another crucial consideration for companies when selecting their insurance provider is whether the prospective partner has the capacity to deal with a sudden influx of claims. If it does not, this can slow down the claims process.

"If an insurer suddenly gets an unusually high volume of claims as a result of a large-scale incident, it becomes a capacity issue and the insurer has to be able to respond to that scenario, they need to have a plan in place," explains Marc. "The insurer needs to be able to create capacity by diverting more internal staff into that area and also making sure they have external loss adjustors diverting to that area."

John cites the example of the devastating earthquake that hit Mexico in September 2017 as a best practice example of how insurers should respond in the early hours and days after a catastrophic event. "Following the earthquake we received 1,400 claims and within 10 days we had physically inspected two thirds of the losses," says John. "We used drones for a lot of the inspections and quickly deployed loss adjustors to the area. In property and CAT claims the early days are key so insurers have to manage their supply chain and get boots on the ground as quickly as possible so that they can support the policyholder."

Photography: Alamy, Reuters Pictures

The right cover

While companies will have certain expectations of their insurance providers, policyholders also have responsibilities. "There are claims that are covered and claims that are not covered so policyholders need to make sure they have the right coverage in place to pick up the exposures they face," says John. The critical word to use here is 'appropriate', says Rob. "While it is impossible to predict where and when disaster will strike, it is of course possible to estimate the potential impact for a company and to buy the appropriate insurance cover with the required limits," he says.

"Recent events have again exposed deficiencies in insurance coverage, with many business owners experiencing losses not directly related to actual property damage, and therefore often outside of the scope of their existing policies. It is critical that business owners are continually re-evaluating their insurance policies to ensure that they match their exposures, both in terms of physical assets and the potential financial fallout resulting from both damage and non-damage-related disruption.

There are also some physical steps that can be taken to limit damage caused by catastrophic events. For instance, flood defence barriers can be put in place if buildings are on a flood plain, and it is advisable to chop down trees and vegetation in close proximity to premises in areas regularly affected by wildfires.

It is also important for companies to have a catastrophe plan so that everyone knows what steps to follow should an incident occur. One way of creating a robust plan is to simulate a catastrophic event to assess what the fallout might be. "At Chubb we simulate CAT events for policyholders," says John. "What we try and do is say: if this CAT event happens this is what it would mean for your business and these are some of the things that you need to consider as a business to respond to that event. It's about planning for an event as a business in partnership with your insurer so that, if the worst happens, you're clear on what you need to do and what your insurer will do."

Careful forward planning can minimise some of the damage caused by a catastrophic event, but it is not always possible to control the uncontrollable. "You can try and mitigate, and you should try and mitigate, but ultimately these events are driven by the power of nature, so as much as you can plan against them, sometimes they are so extreme you are in the lap of the gods," says John. That is why it is so important to have a strong insurance partner. ■

Top five tips for risk managers

1. Policyholders can mitigate against certain risks with preventative measures such as installing flood barriers or clearing vegetation from near premises.
2. For catastrophic events, early notification is critical to a smooth claims process.
3. All businesses should create a 'CAT' plan detailing what steps to follow when an incident occurs and who is responsible for what.
4. It is important to check the right coverage is in place for the exposures faced.
5. Seek out an insurance provider that has experience of dealing with catastrophic losses. Ask whether they have regional catastrophe plans in place and sufficient resources to respond to major incidents in the area, as well as technology such as drones to assess damage in difficult- to-reach areas.

Get in touch

For information on how Chubb handles claims, contact John Latter at John.Latter@Chubb.com or Marc Scheidegger at Marc.Scheidegger@Chubb.com

A risky revolution

The industrial internet of things comes with the possibility of great rewards, but also risk. **Paul Rubens** finds out what cover operators should have in place

The industrial internet of things (IIoT) promises a revolution in the way that companies carry out their business, offering the possibility of huge improvements in efficiency, customer satisfaction and profitability. It is a wave of technology that is likely to become a tsunami as companies adopt it in increasing numbers: consultancy firm Accenture predicts that the IIoT will add more than $14 trillion to the global economy by 2030, and PwC warns that manufacturers that do not transition to the IIoT will be left behind.

For now, the use of IIoT technology is relatively limited: Gartner estimates that about two-thirds of the 8.4 billion "things" in use at the end of 2017 were consumer devices, such as smart TVs and thermostats. That leaves about 1.5 billion "cross-industry" IIoT things, such as those used in smart buildings (including LED lights and security systems) and a similar number of "vertical specific" IIoT devices like process sensors for electrical generating plants and real-time location devices for healthcare. It expects these numbers to more than double by 2020.

So what exactly is IIoT technology? At the simplest level, it consists of a wide variety of things, usually sensors, which collect data (and which may also be able to control nearby devices) for commercial purposes. These sensors are connected to the internet, and they feed the vast volume of data they collect to a central corporate database where it can be analysed, and used in a huge variety of ways. Typical sensors include cameras, thermometers, location trackers (such as GPS devices) and smart meters.

It is impossible to predict precisely how IIoT technology may be used in the future, but it is already being used by companies involved in many industries. For example, engine manufacturers are placing sensors in their products to monitor specific components and alert them when that component is likely to fail or needs to be serviced. Other companies use sensors to monitor temperature in goods containers or to detect the presence of toxic gases in work environments. Sensors also track shipping consignments, optimising the routes that these goods take so fuel consumption can be minimised.

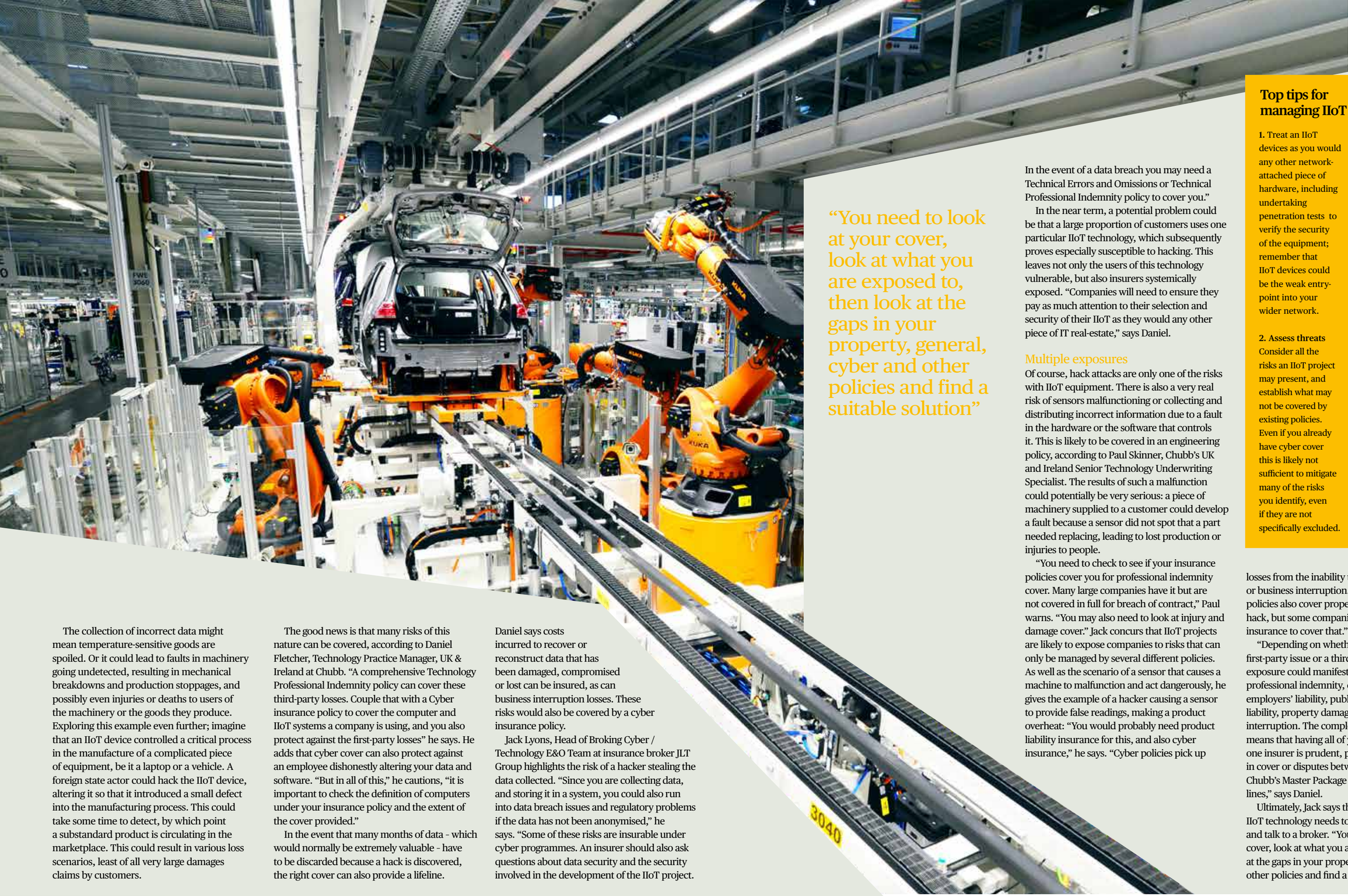
But as well as opportunities, IIoT may also introduce new risks to businesses, and these risks need to be managed to ensure that IIoT applications are successful.

New or old risk?

So, the big question for any company considering integrating IIoT devices is whether those risks are really new, or whether they are simply different manifestations of existing risks. If it is the former, then new insurance policies may be needed to manage that risk. But if it is the latter, then these risks may already be covered by existing policies.

One obvious risk presented by IIoT devices such as remote temperature-monitoring sensors is that they could be hacked; they may be running insecure firmware that leaves them vulnerable to hackers. It is possible that in doing so, a hacker could either compromise some other part of a company's IT infrastructure or alter the way the sensors work. ▶

Photography: Getty Images



The collection of incorrect data might mean temperature-sensitive goods are spoiled. Or it could lead to faults in machinery going undetected, resulting in mechanical breakdowns and production stoppages, and possibly even injuries or deaths to users of the machinery or the goods they produce. Exploring this example even further; imagine that an IIoT device controlled a critical process in the manufacture of a complicated piece of equipment, be it a laptop or a vehicle. A foreign state actor could hack the IIoT device, altering it so that it introduced a small defect into the manufacturing process. This could take some time to detect, by which point a substandard product is circulating in the marketplace. This could result in various loss scenarios, least of all very large damages claims by customers.

The good news is that many risks of this nature can be covered, according to Daniel Fletcher, Technology Practice Manager, UK & Ireland at Chubb. "A comprehensive Technology Professional Indemnity policy can cover these third-party losses. Couple that with a Cyber insurance policy to cover the computer and IIoT systems a company is using, and you also protect against the first-party losses" he says. He adds that cyber cover can also protect against an employee dishonestly altering your data and software. "But in all of this," he cautions, "it is important to check the definition of computers under your insurance policy and the extent of the cover provided."

In the event that many months of data – which would normally be extremely valuable – have to be discarded because a hack is discovered, the right cover can also provide a lifeline. Daniel says costs incurred to recover or reconstruct data that has been damaged, compromised or lost can be insured, as can business interruption losses. These risks would also be covered by a cyber insurance policy.

Jack Lyons, Head of Broking Cyber / Technology E&O Team at insurance broker JLT Group highlights the risk of a hacker stealing the data collected. "Since you are collecting data, and storing it in a system, you could also run into data breach issues and regulatory problems if the data has not been anonymised," he says. "Some of these risks are insurable under cyber programmes. An insurer should also ask questions about data security and the security involved in the development of the IIoT project.

"You need to look at your cover, look at what you are exposed to, then look at the gaps in your property, general, cyber and other policies and find a suitable solution"

In the event of a data breach you may need a Technical Errors and Omissions or Technical Professional Indemnity policy to cover you."

In the near term, a potential problem could be that a large proportion of customers uses one particular IIoT technology, which subsequently proves especially susceptible to hacking. This leaves not only the users of this technology vulnerable, but also insurers systemically exposed. "Companies will need to ensure they pay as much attention to their selection and security of their IIoT as they would any other piece of IT real-estate," says Daniel.

Multiple exposures

Of course, hack attacks are only one of the risks with IIoT equipment. There is also a very real risk of sensors malfunctioning or collecting and distributing incorrect information due to a fault in the hardware or the software that controls it. This is likely to be covered in an engineering policy, according to Paul Skinner, Chubb's UK and Ireland Senior Technology Underwriting Specialist. The results of such a malfunction could potentially be very serious: a piece of machinery supplied to a customer could develop a fault because a sensor did not spot that a part needed replacing, leading to lost production or injuries to people.

"You need to check to see if your insurance policies cover you for professional indemnity cover. Many large companies have it but are not covered in full for breach of contract," Paul warns. "You may also need to look at injury and damage cover." Jack concurs that IIoT projects are likely to expose companies to risks that can only be managed by several different policies. As well as the scenario of a sensor that causes a machine to malfunction and act dangerously, he gives the example of a hacker causing a sensor to provide false readings, making a product overheat: "You would probably need product liability insurance for this, and also cyber insurance," he says. "Cyber policies pick up losses from the inability to use equipment or business interruption. And some cyber policies also cover property damage after a hack, but some companies use property insurance to cover that."

"Depending on whether the claim is a first-party issue or a third-party one, IIoT exposure could manifest itself in a claim under: professional indemnity, cyber insurance, employers' liability, public and products liability, property damage, or business interruption. The complexity of the risk means that having all of your policies with one insurer is prudent, preventing any gaps in cover or disputes between insurers. Indeed, Chubb's Master Package combines all of these lines," says Daniel.

Ultimately, Jack says that anyone integrating IIoT technology needs to assess all the new risks and talk to a broker. "You need to look at your cover, look at what you are exposed to, then look at the gaps in your property, general, cyber and other policies and find a suitable solution." ■

Top tips for managing IIoT risks

1. Treat an IIoT devices as you would any other network-attached piece of hardware, including undertaking penetration tests to verify the security of the equipment; remember that IIoT devices could be the weak entry-point into your wider network.

2. Assess threats
Consider all the risks an IIoT project may present, and establish what may not be covered by existing policies. Even if you already have cyber cover this is likely not sufficient to mitigate many of the risks you identify, even if they are not specifically excluded.

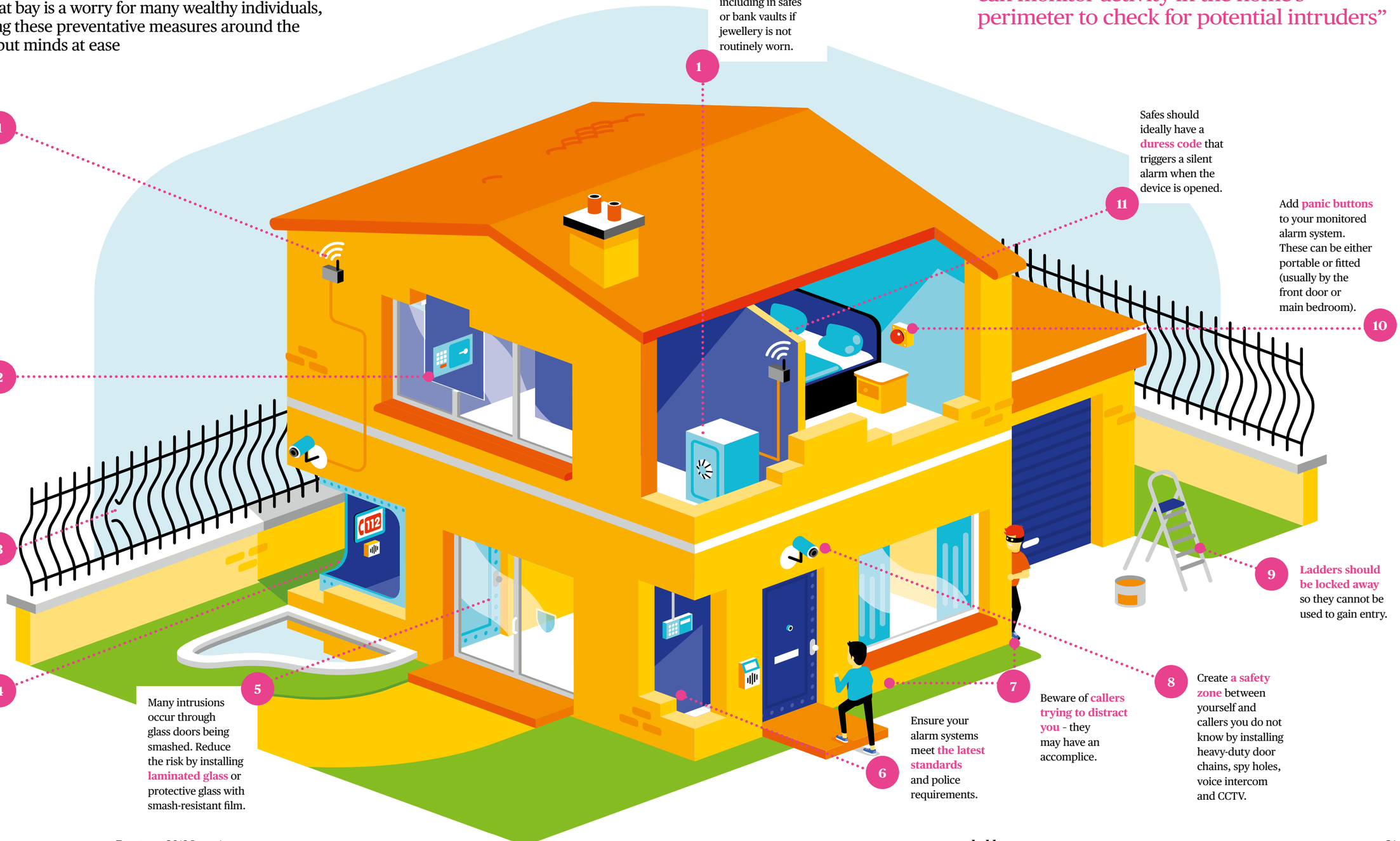
3. Consider bespoke data policies
These could cover items such as IIoT data stores, as well as the risk that the loss, or the corruption, of this data could seriously disrupt your business or cause a complete shutdown for a considerable amount of time.

4. Get risk advice from your broker
An IIoT project may present completely new types of risks that have never before been relevant to your business. Your insurance broker can help you ensure that all such risks are explicitly covered in all relevant policies.

Safe house

Keeping thieves at bay is a worry for many wealthy individuals, but implementing these preventative measures around the home can help put minds at ease

"Skilled operatives at the control centre can monitor activity in the home's perimeter to check for potential intruders"



1 **Valuables should be kept away from public view,** including in safes or bank vaults if jewellery is not routinely worn.

1 Install **remote-monitored CCTV surveillance.** Skilled operatives at the control centre can monitor activity in the home's perimeter to check for potential intruders. They can audibly warn the would-be intruder to remove themselves from the property and notify the authorities of a potential attack.

2 Consider having **two safes – one to 'give up'** that contains less precious items.

3 **Holes in fences** should be repaired.

4 Consider creating a **panic or refuge room** – a secure room linked to the alarm system, with a dedicated phone line.

5 Many intrusions occur through glass doors being smashed. Reduce the risk by installing **laminated glass** or protective glass with smash-resistant film.

6 Ensure your alarm systems meet **the latest standards** and police requirements.

7 Beware of **callers trying to distract you** – they may have an accomplice.

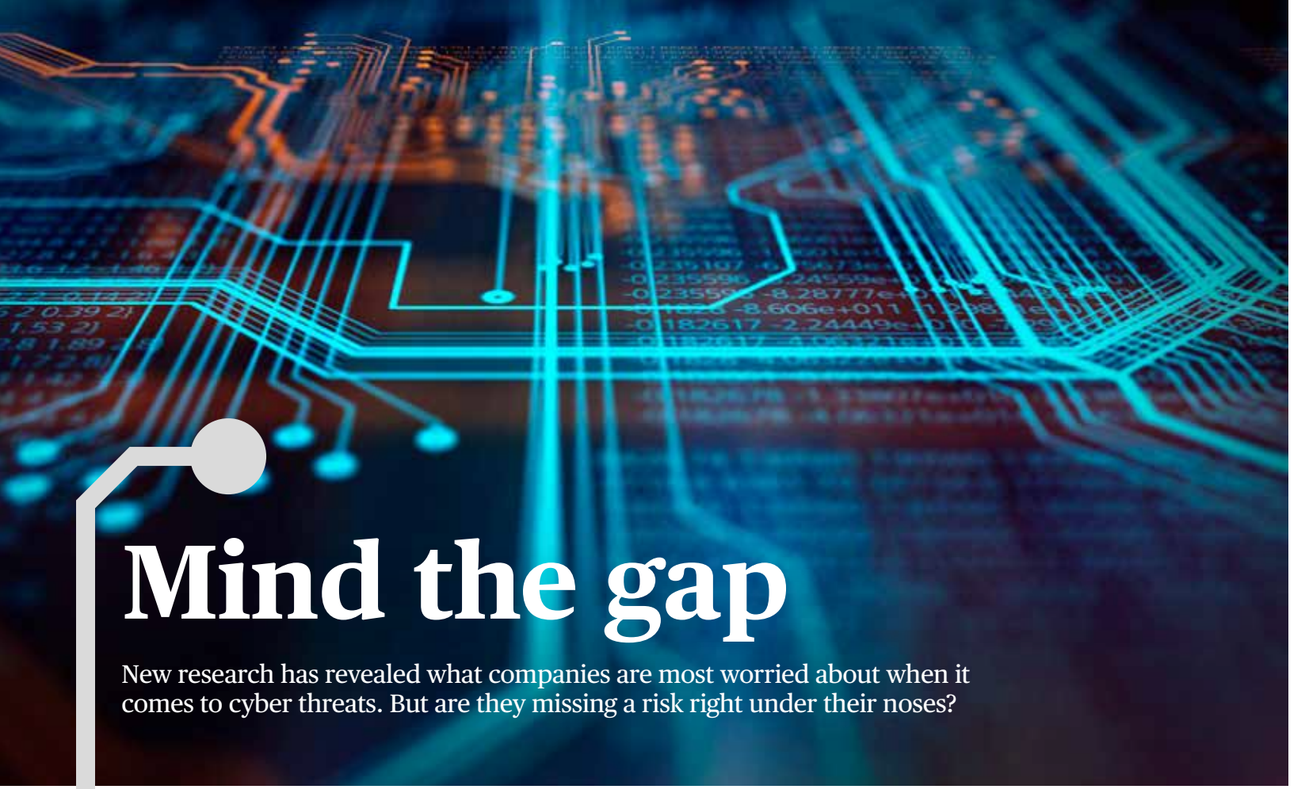
8 Create **a safety zone** between yourself and callers you do not know by installing heavy-duty door chains, spy holes, voice intercom and CCTV.

9 **Ladders should be locked away** so they cannot be used to gain entry.

10 Add **panic buttons** to your monitored alarm system. These can be either portable or fitted (usually by the front door or main bedroom).

11 Safes should ideally have a **duress code** that triggers a silent alarm when the device is opened.

Illustration: Patswerk



Mind the gap

New research has revealed what companies are most worried about when it comes to cyber threats. But are they missing a risk right under their noses?

Businesses may well have cyber attack response plans and policies that kick in when an incident occurs, but a survey of 250 companies across Europe has found that not everyone is fully aware of their responsibilities. Fewer than half of those who have suffered a notable cyber incident agree that everyone involved in the response knew what to do and that it went ahead as planned, according to the research published by Chubb in the report *Bridging the cyber-risk gap*.

The most significant factor in a business's ability to limit the damage of a cyber event is how quickly it can respond. Yet the survey found that many companies are not confident that their incident response plans are up to scratch, or that they test and update them regularly. Worryingly, 55% say their organisation assumes it will never suffer a serious cyber incident. Equally concerning, as Kyle Bryant, Cyber Risk Manager for Europe at Chubb, notes: "Most conversations about cyber risk happen after an event, when obviously, they should be held long beforehand."

To contain an incident effectively, it is crucial that there is a strategic response. A key step, maintains Kyle, is to ensure that a company's defence policy is the clearly defined responsibility of a single individual. "The lead could be taken by any of the departments for which it is a concern – IT, human resources, operations, risk management or the C-Suite. But whichever department is in charge is less important than the fact that there clearly is *someone* in charge."

It's good to talk

With the leadership role established, the next step, says Kyle, is to tackle what he calls "the great divide" between risk management and IT. Only 35% of companies surveyed for the report believe their organisation has good cross-departmental collaboration; and 18% concede that collaboration only happens in response to an imminent threat or following an attack. "To create consistency across the organisation, you have to start in the C-suite," says Kyle. "You need a person of influence across the organisation who can break down the silos and ensure that cyber is treated as an enterprise risk."

Understanding each other better will help bridge the divide, which is often at its widest when comes to how severe people estimate the risk to be. IT professionals are more concerned about the impact of a cyber event than their counterparts in the risk function. This divergence of views on the scope of the threat and how to tackle it can leave companies vulnerable.

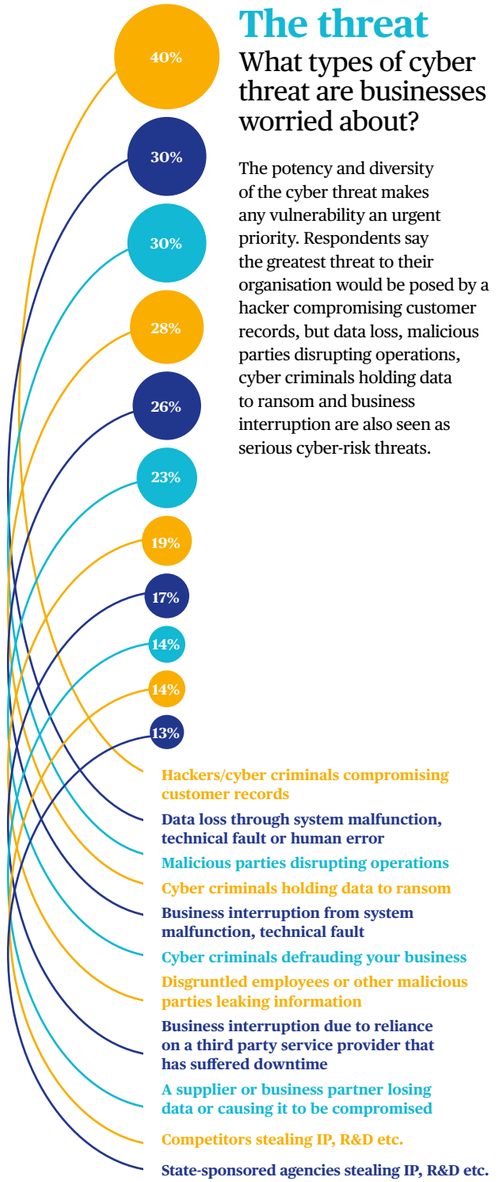
"The reality is that many organisations find it extremely difficult to quantify the potential consequences of a cyber incident or attack," explains Leon Adeyemi, a Chubb London Cyber Underwriter. "IT and risk are going to have to work together holistically to look at the various threats their organisations face and to assess the financial implications of such exposures. Taking a more joined-up approach to risk management represents an organisation's best chance to mitigate the danger effectively."

Emphasising the need for better internal communication, Kyle points to a recent report from AIRMIC, the risk management and insurance organisation. "It observed that risk managers have to become more technically savvy. And IT managers can't be in a silo of their own. Countering cyber attacks is a people process as well as technical process."

The threat

What types of cyber threat are businesses worried about?

The potency and diversity of the cyber threat makes any vulnerability an urgent priority. Respondents say the greatest threat to their organisation would be posed by a hacker compromising customer records, but data loss, malicious parties disrupting operations, cyber criminals holding data to ransom and business interruption are also seen as serious cyber-risk threats.

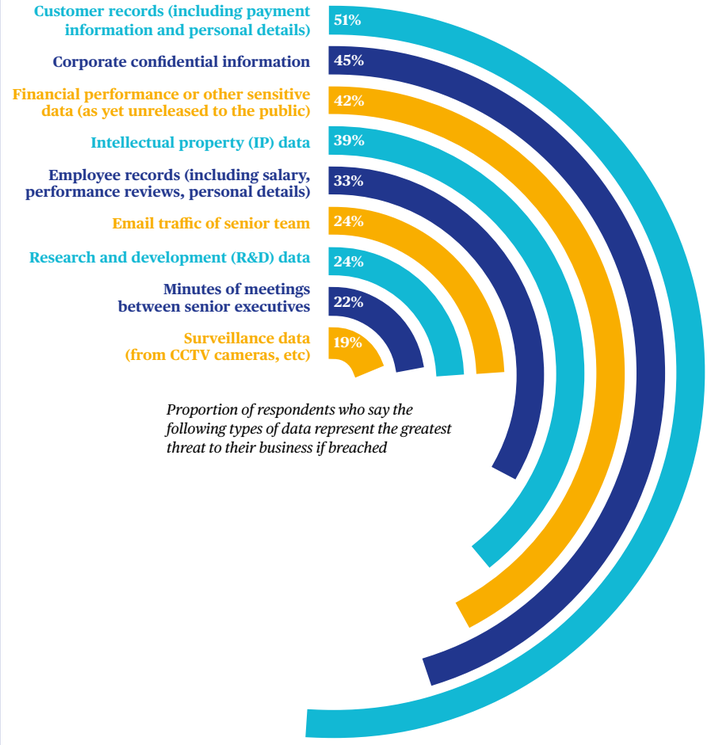


Respondents who believe these factors pose the greatest threat to their business (%)

The risk

What types of data are businesses most worried about?

More than half of respondents say that their customer records, out of all the data they hold, pose a significant risk in the event of a data loss. This could be because this data is a particular focus of the EU's General Data Protection Regulation (GDPR), which recently came into force, along with tough new penalties for organisations that fall foul of the rules – a €20m fine or 4% of global turnover, whichever is greater.



Proportion of respondents who say the following types of data represent the greatest threat to their business if breached

42%

of respondents say that data pertaining to financial performance or other sensitive data, which is unreleased to the public, represents the greatest threat to their business if breached

The vulnerability

Where is the weakest link in cyber defences?

Compared with their colleagues in risk, IT professionals tend to be more concerned about 'the bad actors': 42% cite the sophistication of hackers as worrying, compared with only 27% of their counterparts in the risk function. This is unsurprising: IT professionals are likely to be most aware of the evolving sophistication of hackers and the technologies they use to breach security. This knowledge appears to be increasing their wariness.

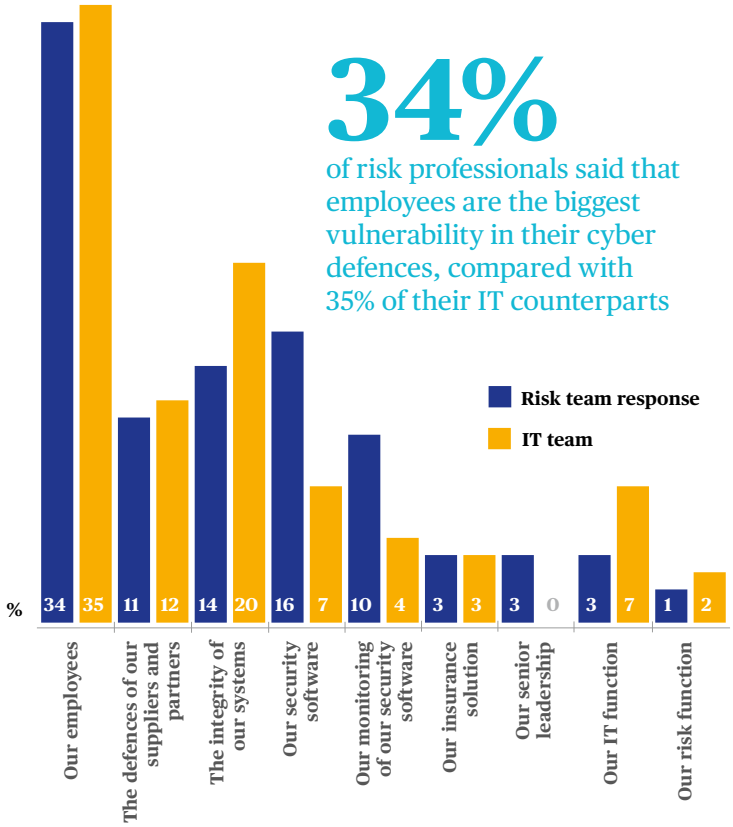
Yet both IT and risk should be looking closer to home: the workforce must be a clear priority for many organisations; 34% of risk respondents and 35% of IT respondents cited overall employee behaviour as the weakest link in their cyber defences. This was, by far, the biggest 'weak link' from both.

A fifth of IT professionals said that the integrity of their systems was the second-most cyber defence weakness, but those involved in risk said it was a business's security software, highlighting risk's inherent lack of faith in the technology they have defending them; 10% also said the monitoring of security software was a cyber risk, compared with 4% of their IT contemporaries.

Conversely, IT saw themselves and risk as more of a danger than risk did.

34%

of risk professionals said that employees are the biggest vulnerability in their cyber defences, compared with 35% of their IT counterparts



The impact

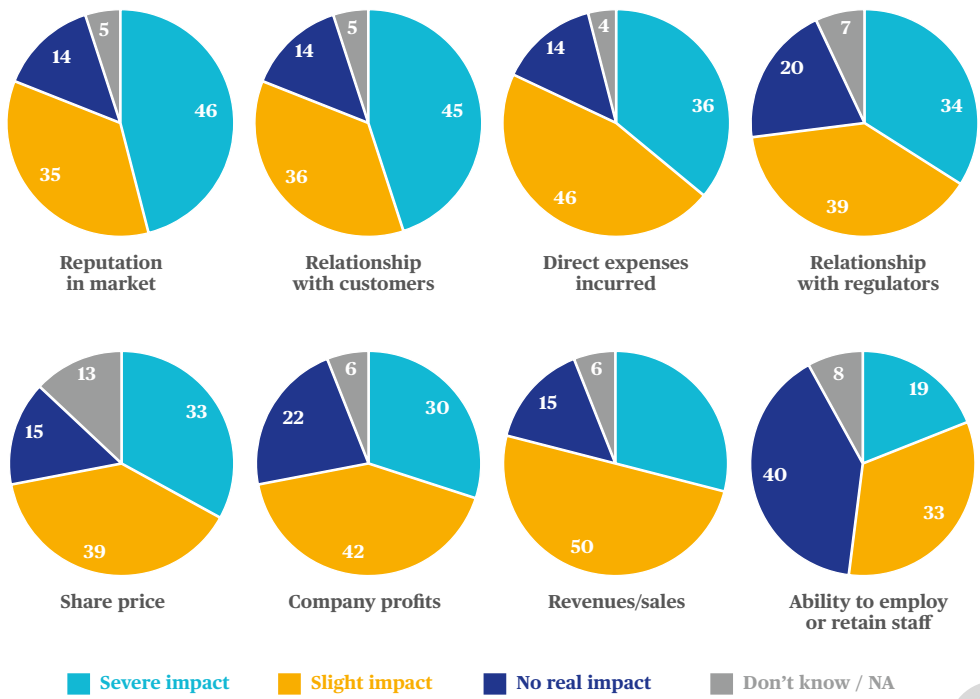
How would a worst-case attack affect the business?

The survey found that IT professionals are more likely than their counterparts in the risk function to expect the impact of a cyber event to be severe. This is further evidence that not all organisations have reached a single view of the scope of the threat or how to tackle it, which can leave them vulnerable.

When asked what the fall out from an attack would be, 46% said market reputation would be severely affected. Just behind was the business's relationship with customers, cited by 45%, followed by the direct expenses incurred, said by 36%.

At the other end of the scale, 40% said there would be no real impact on the ability to employ or retain staff in the event of a cyber attack. ■

% of Respondents



45%

of respondents believe that a cyber attack would severely affect their business's relationship with customers

Real estate risk

Property is a popular choice for investors but how can they keep their portfolios safe?

Risk and uncertainty pervade the real estate sector like few others. Construction companies face pressure to deliver on time and on budget, businesses must deal with complex regulations and leases, and investors worry about income and capital returns.

Choosing which property to buy can be devilishly difficult, not only for a couple buying their first home, but also for a company searching for new offices. Indeed, in real estate "everything is relevant", as David Geltner, Professor of Real Estate Finance at Massachusetts Institute of Technology (MIT), has said.

But in an industry where everything matters, how can you effectively identify and mitigate risks? This is an important question for investment funds, pension funds and other large property investors, as well as owner-occupiers.

Idiosyncrasies amid the boom

Investment in real estate hit a record high of $1.62 trillion (€1.42 trillion) in 2017, up from $1.43 trillion the previous year, according to Cushman and Wakefield's Global Investment Atlas. Asian investors were the biggest driver of the rise and London remained the most sought-after city.

While the appetite for real estate is clear, attempts to forecast returns are shrouded in uncertainty. Investors need to make an array of assumptions not only about the physical assets but also about the wider property market. Furthermore, while classifying properties by sector and region may seem natural, neither provides a sound basis for risk reduction.

"Spreading a portfolio across sectors or regions does not work very well because these factors don't explain enough of the difference

between properties," said Tony Key, Professor of Real Estate Economics at Cass Business School in London. "Simply buying more assets is effective, however, because so much of the risk is related to idiosyncratic differences between buildings."

Heavy exposure to just one region may call for some diversification, but so would bunching of lease termination dates. Studies suggest that holding between 30 and 50 properties substantially reduces risk. But full risk diversification requires a portfolio of 200 properties or more.

The UK's Investment Property Forum has suggested that while there "may be no silver bullet" for portfolio risk, new approaches could enable better future management.

Salient risks

Many corporations are owner-occupiers of large amounts of real estate. These businesses are sure to consider cost and convenience when deciding where to buy or build offices, warehouses and retail spaces.

But what about risks that could severely disrupt business operations? Globally, the annual average of 335 weather-related disasters per year between 2005 and 2014 was 14% higher than in the previous decade, according to the United Nations.

Yet businesses and investors could receive far more detailed insights into climate and weather-related risks to real estate than is currently the norm. A 2017 report for the UK-based Royal Institution of Chartered Surveyors (RICS) looked at flood risk management across commercial property in Australia, China, Germany, the UK and the US. It found "substantial potential" to increase the role of built environment professionals – who deal with creation and modification of, for example, buildings, parks and transportation systems – in mitigation and called for a better understanding of how climate change is altering the risk. The report also suggested legislation could encourage insurance uptake in flood-prone areas.

In addition to the traditional risks associated with floods, earthquakes and windstorms, there are newer risks that real estate owners should consider. Piers Gregory, Head of Terrorism and Political Violence at Chubb, explains: "The threat of terrorism has evolved significantly in recent years and has become increasingly difficult to predict. Traditionally the target for terrorists has been large iconic buildings or government owned assets but the impact is being more widely felt with mass casualties and high media impact often being a key objective. This means all industry sectors can be impacted whether directly or indirectly. The appropriateness and relevance of terrorism insurance should be a key consideration, especially for those operating within high density areas such as central business districts.

Adding to this is the real possibility that facilities could be paralysed by cyberattacks that encrypt or lock files. Hackers have also shown that smart thermostats could be hijacked to fix the temperature at an unbearable level until a ransom is paid. Karen Strong, Head of Industry Practices UK and Ireland at Chubb, says: "There is an urgent need to ensure that adequate cyber security is in place alongside post-data breach recovery plans. Real estate companies have high transaction volumes and values and have responsibility for sensitive data – data that would be valuable to other parties. They are further exposed to cyber threats nowadays due to the many parts of a building that are becoming internet enabled. If any of these things are compromised in any way, they can have a significant impact on the trading reputation and business continuity of the real estate company."

The life stages of buildings

Demand for technical due diligence reports on the physical condition of buildings has been increasing in Europe. With the globalisation of the real estate market, financial institutions, investors and owner-occupiers want a better understanding of what they are buying and selling. Professor Geltner undertook research that found commercial buildings in the US tend to last around a century. This 'lifetime' can be divided into three stages: 'youth', which lasts 30 years and involves a sharp initial drop in value; 'middle age', during which buildings may need more maintenance but their values vary relatively little; and 'old age', whereby values decline rapidly after 65 years since construction.

Together, this decline and spending on routine improvements amount to annual 'gross depreciation' of 7% of a building's remaining value, according to MIT. Professor Geltner says this is higher than the real estate investment industry generally assumes.

Whatever a building's age, surveyors and risk engineers can assess any hazards and help prevent or minimise business interruptions. Risk engineering experts can not only identify and quantify risk areas but also develop smart and pragmatic solutions to technical issues and health and safety challenges.

"Whatever a building's age, surveyors and risk engineers can assess any hazards and help prevent or minimise business interruptions"

Digital technology is helping risk professionals hone their approach in a range of areas. For example, building control surveyors can use 3D digital models to manage fire safety plans.

But technology cannot replace a risk engineer who understands the local laws, codes, standards, customs and language, and will be able to offer bespoke solutions. Whether they are looking at machinery, water supply, fire safety or anything else, risk engineers must be attuned to the details that make all the difference. In this respect, their expertise offers lessons for anyone with a stake in real estate. Remember that everything is relevant, that risk can be reduced but not removed, and focus on what you can control. ■

This content was produced by the advertising department of the Financial Times*, in collaboration with Chubb*

Get in touch

For more information contact Karen Strong at kstrong@chubb.com and Piers Gregory at piers.gregory@chubb.com

Play to the whistle

Regulators are looking to encourage whistleblowing and self-reporting, with important implications for directors, says **Stuart Collins**

Illustration: Andy Martin

Whistleblowers are not always viewed favourably in the corporate world, but increasingly they are playing an important role in addressing corporate wrongdoing. In recent years, whistleblowers have been central to some of the most high-profile regulatory investigations, several of which have resulted in large settlements, fines and even criminal prosecutions.

Statistics suggest that whistleblowing is on the rise. An international survey of business managers by law firm Freshfields Bruckhaus Deringer found that 47% had witnessed or engaged in whistleblowing, up from 34% in 2014.

Regulators are a major driver of this trend, although many companies also now see it as a way to root out unacceptable behaviour, such as fraud, bullying and harassment, or the flouting of safety or environmental rules. In recent years the US has embraced whistleblowers, and as a result European companies with US listings have seen the introduction of tough whistleblowing requirements and protections under a number of regulations, including the Sarbanes-Oxley Act and Dodd-Frank.

The US has turned whistleblowing into an effective regulatory tool. Under the Securities and Exchange Commission (SEC) whistleblower programme, those who come forward can receive 10% to 30% of SEC settlements and fines if their information leads to a successful action that results in sanctions in excess of $1 million (€1.1 million).

In March 2018, three whistleblowers shared an $83 million award following a successful SEC prosecution of a Wall Street bank. Since the programme began in 2011, some 57 whistleblowers have received $320 million in awards, according to SEC statistics.

The SEC recently announced its intention to improve incentives for whistleblowers under its seven-year-old programme. In proposals published in June, the regulator says it plans to increase payouts for smaller cases, and limit awards for large settlements.

US derivatives regulator, the Commodity Futures Trading Commission (CFTC), also recently reported an increase in awards paid to whistleblowers. Before 2018, the CFTC had issued just four whistleblower awards amounting to less than $11 million. In July the Commission granted three more, totalling over $75 million, including a $30 million award paid to a whistleblower, the largest to date under the CFTC's Whistleblower Program.

Daisy Laskey, Regional Financial Institutions Manager at Chubb, says whistleblowing in Europe is in its infancy compared with the US, but that is changing. She notes that a number of European countries have introduced tougher whistleblowing requirements to encourage the reporting of corporate wrongdoing.

France and Italy have introduced legislation requiring companies to put whistleblowing procedures in place, as well as introducing protections for people who speak out. The Freshfields Bruckhaus Deringer survey found that business managers in France are now the most likely among all countries to be involved in whistleblowing.

In the UK, the 2016 Senior Managers Regime introduced requirements on banks aimed at encouraging employees to speak out, and increased protections for employees that raise concerns. The UK's Competition and Markets Authority (CMA) now offers whistleblowers a reward of up to £100,000 for information on cartels, as well as promising them anonymity.

In Europe, whistleblowing protections are less well developed. Only 10 EU member states currently ensure that whistleblowers are fully protected, according to the European Commission. However, in April the EU proposed new laws to strengthen whistleblower protection across the EU.

The Commission wants to establish an EU-wide standard to establish safe channels for reporting breaches of EU law, as well as to protect whistleblowers from retaliation. Under the proposal, all companies with more than 50 employees or with an annual turnover of more than €10 million will have to set up an internal procedure to handle whistleblowers' reports.

> "As regulators have taken steps to encourage whistleblowing, we have witnessed an uptick in investigations and claims against D&O insurance. This is leading to an increase in liability"

Growing risk

The desire to hold directors to account, together with the growing interest in whistleblowing from regulators, is leading to an increased exposure for executives and boards, Daisy believes. "As regulators have taken steps to encourage whistleblowing, we have witnessed an uptick in investigations and claims against D&O insurance. This is leading to an increase in liability and is of material concern to D&O insurers and policyholders alike," she says.

Generally, whistleblowing takes one of two routes. The whistleblower can go direct to the regulator, or they can follow the internal whistleblowing procedure of the company, and the company can then go to the regulator. The route taken has important consequences for D&O cover.

Internal investigations are typically not covered by most D&O policies, explains Kurt Rothmann, Senior Partner in the Financial Lines Group at brokers JLT Specialty Ltd. "D&O policies tend to trigger following a self-report to a regulator in relation to a suspected or actual breach of legal or regulatory duties. However, insurers are generally reluctant to trigger cover if there is an internal investigation by a company ahead of a self-report being made, although they may agree to language that provides cover retrospectively if a self-report is actually made," he says. ▶

Insurers, including Chubb, have been amending D&O policies to take into account whistleblowing and the resulting internal investigations. For example, some D&O policies have been extended to include the costs incurred by individual directors during internal investigations conducted by the company when a self-report is made to a regulator (such costs were previously excluded by D&O policies).

According to Daisy, cases tend to be fact-specific and play out differently depending on the jurisdiction, the allegations, the regulators involved and where they are located, and the identity of the whistleblower (it could be a director). However, companies can work with their D&O insurers and brokers to ensure that policies will respond appropriately to different scenarios.

"Make sure that you know that your D&O policy is fit for purpose for whistleblowing cases. In particular, coverage for directors' legal costs during internal investigations prior to a self-report that is formally made to a regulator should be included, insured vs insured exclusions should allow for whistleblowing by a director and that conduct exclusions will work in a whistleblowing scenario," Daisy explains.

Kurt adds that it is very important to engage with insurers at the appropriate levels within the organisation when making a claim. Careful consideration should be given to the drafting of the notice and subsequent communication. "D&O claims will often involve conflicts between directors sitting on the same board and revolve around serious allegations as to the appropriateness of their conduct," Kurt continues. "Notifying this to insurers in an appropriate manner is an important part of the claims process."

Kurt also advises directors to review their cover and focus on when their D&O cover triggers: "They should ensure they understand how to access the policy directly, as they may find that they are in conflict with their company and employer as a result of a whistleblowing procedure being activated. An adequate programme limit is also essential and should be determined following a detailed assessment of exposure."

> "Inadequate whistleblowing procedures could allow bad behaviour to continue unchecked"

Above all, companies and their directors need to ensure that adequate internal whistleblowing procedures are in place. "Companies need to make sure that the right controls are in place and tested, and make sure that employees are made aware of the whistleblowing procedures," Daisy says.

D&O insurance buyers should also review their excess policy forms, Kurt recommends. They should specifically ensure that these are fully 'follow form', meaning that they mirror the primary policy language and do not introduce any additional terms. This excess policy should also address "how insurers will respond where there is a compromised claims settlement or where the underlying insurers do not respond because of insolvency or policy language preventing aggregation of the limits available to the insured under different policies issued by the same insurer".

Daisy concludes: "Failure to implement internal whistleblowing processes could result in claims against directors for their failure to do so. But inadequate whistleblowing procedures could allow bad behaviour to continue unchecked, eventually resulting in regulatory actions and litigation." ■

D&O coverage tips

- Loss scenarios - carry out whistleblowing loss scenario testing to work out the response of D&O cover.
- Adequate limits - internal and pre-investigation cover will eat into the overall limit, especially where multiple directors are involved in an investigation, each requiring their own legal representation.
- Conduct exclusions - D&Os need to consider clauses that preclude coverage for fraudulent, criminal or wilful misconduct in the context of internal investigations.
- Insured vs insured - exclusions should allow for whistleblowing by a director.
- Discrimination or wrongful termination - these kinds of allegation by the whistleblower against the company are not a D&O exposure, but they can lead to employment practice claims.

Get in touch

For more information on Chubb's director's & officers insurance, contact Daisy Laskey daisy.laskey@chubb.com

Cyber defences

Preventing criminals from getting their hands on data is a top priority for businesses globally. So what actions should be on their agendas?

Cyber security is a growing priority for businesses worldwide amid rising concerns about the impact of hacking and data breaches. Estimates suggest cyber crime may cost the global economy more than $400 billion (€349 billion) every year and the global reach of ransomware attacks such as WannaCry has heightened awareness of the threat.

But while the issue is moving up the corporate agenda, the ability of companies to adapt to the fast-evolving nature of the threat is less clear. Businesses differ significantly in how they approach the challenge, according to a new Financial Times Pulse Survey for Chubb.

While almost half said responsibility for cyber security within their business is a company-wide issue, 31% said it is mainly an issue for IT, and 15% said either the Board or the C-suite is held most responsible. The survey, which received 356 responses from across the world, also found:

- Cyberattacks are one of the biggest business risks for 48% of respondents (but the top risk for only 3%)
- Loss of sensitive data was the greatest fear, followed by impact on customer relations and damage to reputation
- Nearly half of companies gave cyber security training to all staff in the past 12 months (rising to 58% in the US)

Building teams, training people

Many businesses fail to identify all their potential cyber risks due to issues with their structure, according to Dr Larry Ponemon, founder of the Ponemon Institute, a US-based information security research centre.

"Cyber strategy starts with good governance," he says. "Sixty per cent of

companies globally are not capable of understanding all their risk areas because they haven't built a security framework."

Dr Ponemon emphasises the need for cyber security to involve "a C-level executive who communicates regularly to the CEO, as well as the board of directors". This executive should have the power to build a team with different skill sets by hiring and firing, he adds.

But such a team cannot make a company secure on its own. Phishing, one of the most common forms of attack, involves social engineering: fooling staff into clicking on malicious links or disclosing information.

More than nine in ten survey respondents agreed or strongly agreed that phishing is a serious threat. In the US, nearly two thirds strongly agreed, compared with under half in Europe, the Middle East and Africa (EMEA).

"Educating rank-and-file employees is a very low-cost way of getting people to do the right thing," explains Dr Ponemon. Businesses also need to beware of 'whaling' attacks, where senior figures receive fraudulent emails that appear to come from trusted sources.

"Employee training is an important factor, reducing the cost of a breach by $12.50 per lost or stolen record"

As Kyle Bryant, Cyber Risk Manager, Europe, at Chubb, puts it: "Ownership of IT security needs to be a cultural thing: no matter what level of an organisation you are at, no matter which silo you are in, it needs to be embedded in what you do."

Strong defences save dollars

A handful of other key factors are also crucial to deterring cyberattacks and limiting the damage of any that do occur. In its annual Cost of Data Breach Study, the Ponemon Institute puts dollar figures on measures that help to contain costs. Employee training is indeed an important factor, reducing the cost of a breach by $12.50 per lost or stolen record.

Two other factors were found to be even more important: extensive use of encryption (saving $16 per record) and having an incident response team in place ($19 per record).

Survey respondents largely understood the value of encryption: 85% agreed or strongly agreed that personal data should always be encrypted. As with phishing, executives in the Americas felt more strongly about this than those in EMEA.

"Encryption goes back thousands of years to the Egyptians," said Dr Ponemon. "It's not new but it helps because when hackers see that a database is encrypted, they tend to look for lower-hanging fruit."

No matter how good your defences, experts warn that successful cyberattacks can never be ruled out. Companies therefore need incident response plans to contain the fallout. A plan should spell out the critical actions to be taken, in which order and who will be responsible for what. Nor can they be confined to a one-size-fits-all approach; a mass breach of customer data will require a very different response to less serious attacks. "Incident response plans need to be a living thing, tested and tailored for each type of incident," says Kyle.

As revealed by Chubb's *Bridging the cyber-risk gap* report (see page 22), many companies that have not been hacked do not have clear plans that they regularly test and update. But complacency might prove costly.

The average total cost of more than 400 data breaches examined in the 2017 Ponemon Institute study was $3.62 million. Companies lacking a rigorous incident response plan usually cannot contain attacks, according to Dr Ponemon. "You have to be ready to respond at the drop of a dime," he adds.

Into the unknown: evolving with risk

The global cyber insurance market was worth $3.5 billion in 2016 but could more than double by 2020, according to the Organisation for Economic Co-operation and Development (OECD). While the US currently dominates the market, growth could be led by Europe.

"Businesses are becoming more aware of stand-alone cyber insurance and take-up rates are increasing," says Steve Simchak, Chair of the Global Federation of Insurance Associations (GFIA) Cyber Risks Group and Director of International Affairs for the American Insurance Association. "It's critical that companies work with their broker to identify gaps in their other insurance policies and understand how much cover they have for cyber risks."

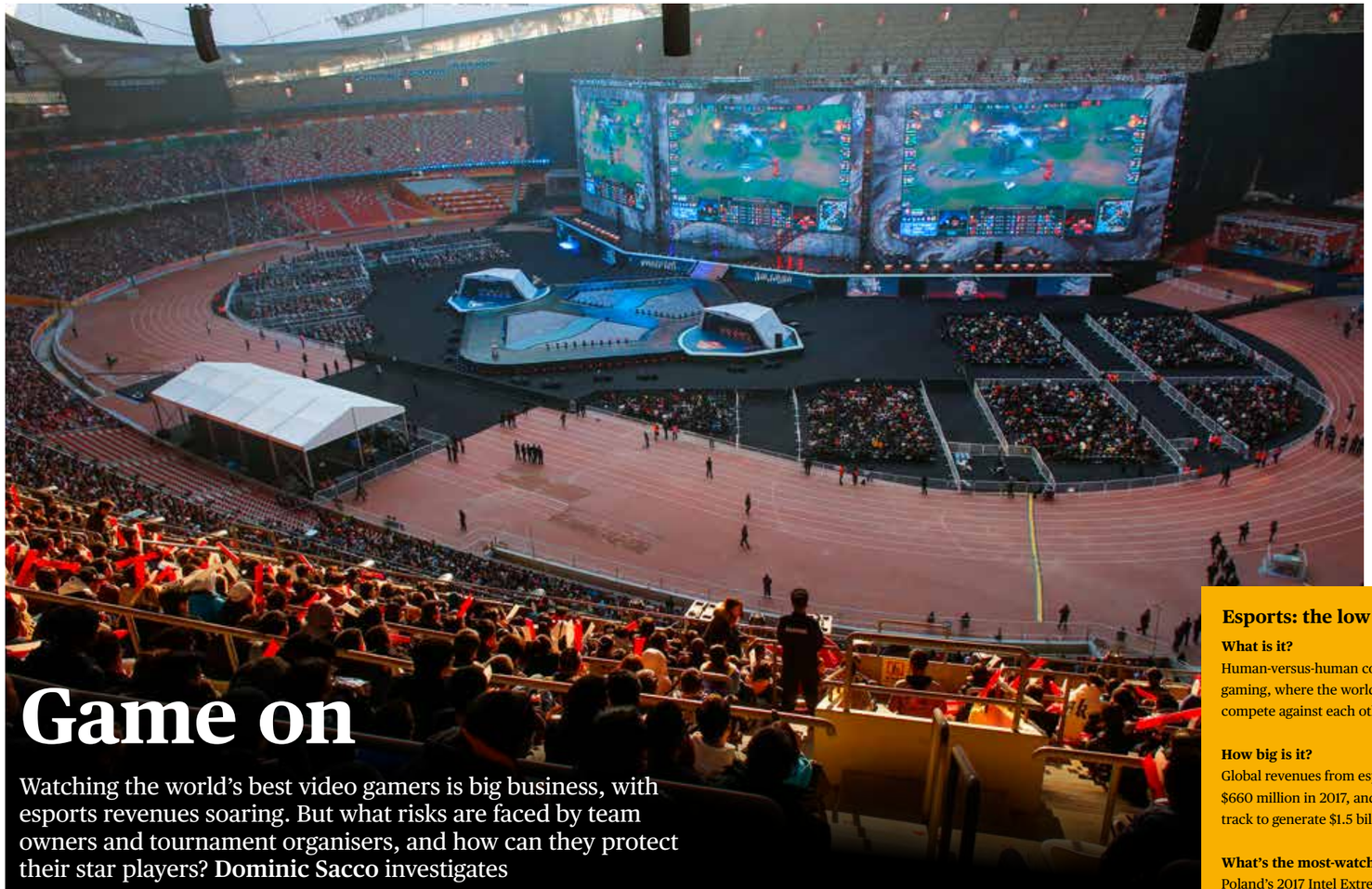
In broader terms, cyber security will continue to be about plugging gaps that hackers could exploit - a task that will only get harder as the internet of things expands.

"Cyber risk is evolving every day, every minute in some cases," says Kyle. "I think the fear of the unknown is something real, it's legitimate and it's completely reasonable. Organisations have to build risk management that evolves with that." ■

This content was produced by the advertising department of the Financial Times*, in collaboration with Chubb*

Get in touch

For information on how Chubb can help you manage cyber risk, email Kyle Bryant at kyle.bryant@chubb.com



Spectators watch the League of Legends 2017 World Championships Grand Final esports match between Samsung Galaxy and SK Telecom T1 at the Beijing National Stadium in Beijing, China

Game on

Watching the world's best video gamers is big business, with esports revenues soaring. But what risks are faced by team owners and tournament organisers, and how can they protect their star players? Dominic Sacco investigates

What began as an underground activity has become one of the most exciting and fastest-growing industries of the 21st century. Esports (aka electronic sports) has become its own separate entity, with different tournaments, professional players, teams and games for fans to follow. It is essentially competitive video gaming, where people play against one another either online or at events in arenas, usually for a cash prize.

Viewers can watch games such as League of Legends and Counter-Strike live online via streaming platforms such as Twitch and YouTube and in person at stadiums, with the biggest esports tournaments pulling in millions of spectators. Esports has even caught the eye of big sports clubs such as Manchester City and Paris Saint-Germain, and brands like Coca-Cola, Samsung and Red Bull.

Global revenues from esports including advertising, sponsorship, ticketing and merchandise rose 33.9% year on-year to $660 million in 2017, according to market analyst Newzoo. This is expected to grow to $1.5 billion in 2020.

But what kind of risks are faced by esports tournament organisers and professional teams in this burgeoning sector?

Wouter Sleijffers, CEO of one of the world s top esports clubs - Fnatic - says an important risk is whether their professional players pick up an injury or fail to turn up at an event.

"In those cases we've been able to tap into contracted substitute players or stand-ins, as long as it's allowed by the rules," he says. "However, in the past, some teams have needed to cancel participation due to visa restrictions or not having enough time to apply for a visa, depending on the origin of the player and location of the event.

Generally speaking, we assess risks on an ongoing basis and work with experienced people internally and externally to minimise risk. In esports specifically, due to the increased stakes, investments and valuations, it's becoming more and more important that we remove any unwanted eventualities and insure ourselves for negative scenarios."

Francis Hernandez, International Entertainment Manager at Chubb, highlights esports player injury as a potential risk. "Injuries can affect the team's performance - if they have to sub someone else in - and the viability of the event," he comments. "Insurance could cover non-appearance but the underwriters would need detailed information, such as medical details."

Emma Bennett, Chubb's Head of Affinity, Employee Sponsored Benefits & Direct Marketing for Accident & Health, agrees: "There's got to be a duty of care. There's a lot of prize money around esports and, because of that, they're going to be looking after the welfare of the people involved in esports, whether it's preventing the likes of carpal tunnel syndrome [a wrist problem] or perhaps poor lifestyle - so ensuring players have regular breaks and proper nutrition."

> "Terrorism insurance is also one of the things we get asked for now"

Personal accident cover could provide affected esports players with a lump sum of around £20,000, depending on the incident. There is also higher-frequency cover that would kick in if the player needed counselling following trauma, for example. However, it is important to note that injuries in esports can be very different to those picked up from physical sports.

Emma explains: "Some of the challenge around writing esports may be the fact that injuries are gradual and may happen over a period of time, for example, wrist injuries caused by repetitive strain injury, as opposed to a single and defined event that can be measured, such as a footballer who tripped, or tried to head the ball and got injured in the process." There are other options available, such as death, disablement and disgrace insurance. So, if a player disgraces him or herself, and their team no longer wants anything to do with them, the club can buy a policy that protects the contract value they would have had to pay that person.

Minimising risk

As with traditional sport, part of the appeal of esports is the fact that almost anything can happen during a match. But because of the live nature of broadcasting, technical problems can arise and streams can go down. It is rare, but entire events can even be cancelled.

For esports tournament organisers such as ESL, the show must go on. ESL UK Managing Director James Dean says working closely with game developers and players is key to minimising risk. "As long as we are working closely with the IP owners, we can work towards player education and understanding - managing their expectations of what opportunity esports presents," he comments. "Educating different industries in an open and honest manner is the best way in which we can minimise the risk for the esports industry."

Prevention is not always the cure, as some unexpected situations may still arise that could result in a loss of earnings or event interruption. And Chubb's Francis Hernandez says, this is where insurers may come in, either offering an annual policy or one-off solutions. "I think the least event organisers should look at doing is to protect their expense exposure, so that if an event does get cancelled for whatever reason, they want to be in a position where their balance sheet ends up at zero again as a bare minimum," he explains. "Something could happen to the venue, for example, it could burn down or have an electrical blackout. Terrorism insurance is also one of the things we get asked for now."

Regardless of the potential pitfalls, esports is in an extremely exciting phase right now. And as the sector grows, the demand for insuring tournaments and players will surely grow along with it. ■

Esports: the low down

What is it?
Human-versus-human competitive video gaming, where the world's best players compete against each other for cash prizes.

How big is it?
Global revenues from esports reached around $660 million in 2017, and the industry is on track to generate $1.5 billion in 2020.

What's the most-watched tournament?
Poland's 2017 Intel Extreme Masters, which included competitions in several games, recorded 46 million unique viewers overall.

What's the biggest prize pool?
The Dota 2 International handed out just shy of $25 million to the best players and teams in the world.

Where to watch?
Twitch is the most popular viewing destination, with more than 100 million people tuning in to watch and chat about live games every month. YouTube, Facebook and developer websites also host matches, while even TV broadcasters such as Sky and the BBC have also dabbled with esports coverage in the past.

Photography: Reuters Pictures

Chaos calls. Calmness answers.

Tarik and Samantha Aziz had a newborn, visiting in-laws and two separate water leak disasters at the same time. Chubb's response gave them peace of mind when they needed it most.

Watch the full story at chubb.com/aziz.

CHUBB®

Chubb. Insured.℠