CHUBB®

2016 Issue 1

Progress

Life in the fast lane

Insuring the cars, jewellery and luxury properties of high net worth individuals

Living in smart cities
How technology is helping to improve living standards and reduce energy consumption

Lessons from Tianjin
What can we learn about accumulation risk from the blast at the Chinese port?

Winds of change
The renewable energy sector is booming, but what are the risks facing the industry?

Welcome

In this first issue of *Progress* to be published under the Chubb name, we introduce our new organisation and hear from managers across our business about the benefits it will bring to our customers.

But this magazine isn't all about us. It's about the risks our clients face and how they can be mitigated. In our feature on smart cities on page 8, for example, we consider the risks of the technology being employed to make city life easier, from drones that spot parking spaces to street lights that collect data.

We also hear from David Ralph, head of risk management and compliance at Hong Kong-based PCCW, about the risks posed by cyber attacks. He tells us that cyber crime has become a safer option for thieves than other types of crime, since many companies do not even know if they have been victims or not.

On page 24 we learn more about the needs of ultra high net worth individuals. The number of people who fall into this category has risen by 60% in a decade and, whether they own super yachts or fine wine collections, their possessions need to be protected.

We've also looked at the amazing world of remote surgery, which enables surgeons to operate on patients who are thousands of miles away. It's fantastic technology, but who is responsible if the equipment fails?

I hope you enjoy reading this edition of *Progress*.

Andrew Kendrick
Regional president, Europe
Chubb

CHUBB®

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

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

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

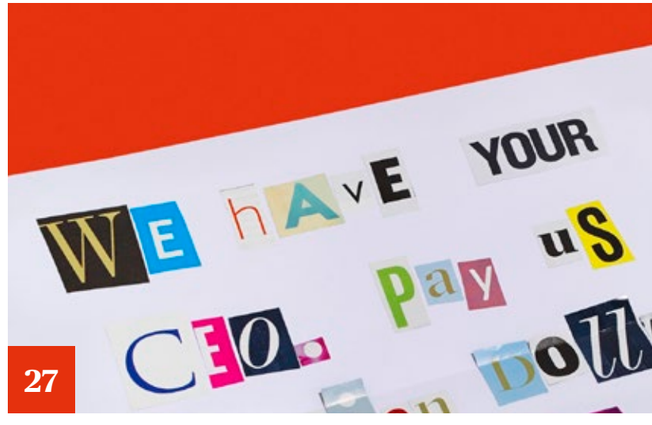
Progress is published on behalf of Chubb by Wardour, 5th Floor, Drury House, 34-43 Russell St, London WC2B 5HA
Tel +44 (0)20 7010 0999
www.wardour.co.uk

Content Director Andrew Strange
Designer Dean Buckley
Account Director Charlotte Tapp
Creative Director Ben Barrett
Managing Director Claire Oldfield
CEO Martin MacConnol

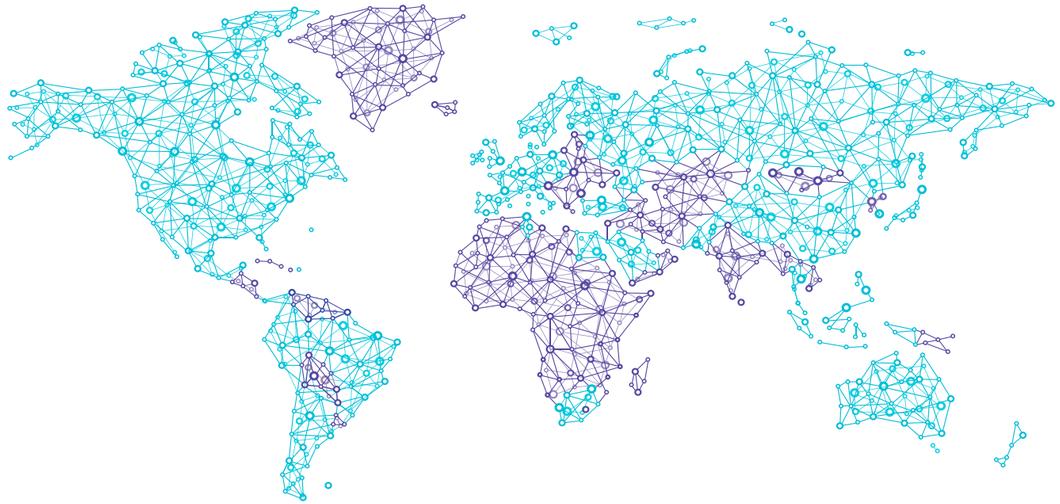
'wardour'

8


16



27



Introducing the new Chubb

ACE and Chubb are now one company and clients are already feeling the benefits of our greater scale and depth

It is now several months since ACE acquired Chubb for US$29.5 billion, creating the world's largest publicly traded property and casualty insurer.

According to Andrew Kendrick, senior vice president, Chubb Group and regional president, Europe, that deal gives the new Chubb "even greater collective know-how and market firepower", which will deliver improved service and innovation.

Among the benefits he highlights is the coming together of complementary businesses - for example, legacy ACE's reputation for its global accounts and multinational leadership plus legacy Chubb's middle market expertise.

Andrew says: "In fact, both companies have experience in these segments and when you put us together that gives us a stronger platform from which to grow - and to help our clients grow."

He adds that the new Chubb is ideally suited to show the discipline needed to navigate today's challenging marketplace conditions. "Only insurers and reinsurers with the willingness and ability to underwrite for profit will be able to prosper and protect their balance sheet for their customers.

"Both our legacy companies were renowned for their strong underwriting cultures. At our core, we are underwriters - we share a passion for the art and science of underwriting. So we share a lot in common when it comes to our underwriting approach and our focus on discipline."

Innovation will also be a priority, says Andrew. "We need to broaden the solutions we provide if we are to remain relevant for our clients in the future."

Already this year, Chubb has announced a new cyber risk service in partnership with Crawford & Company, and Andrew says the company will continue to invest in bringing added-value services to market.

"Chubb has local operations in 54 countries and territories. And in many of those countries, we have extensive branch office networks. While we have a global footprint, we're really a local company everywhere we do business," says Andrew. ■

54
The number of countries where Chubb has operations

30,000
The approximate number of employees worldwide

AA
Our financial strength rating by Standard & Poor's

$55.4bn
Our total capital, which reflects our capacity for risk

Crafting innovative products

The new Chubb has a huge product portfolio, helping businesses and individuals protect themselves from even the most complex risks

At Chubb, we have one of the largest product portfolios in the insurance industry, with more than 200 commercial insurance and reinsurance products and services. These include specialty coverages for clients ranging from multinational corporations, middle market companies and small businesses to consumers.

Our approach to underwriting is fuelled by passion, drive and ingenuity. And it's through superior underwriting that we craft our range of products. These range from specialty and traditional commercial property and casualty for business to personal accident, supplemental health, home and car insurance, personal line and other specialty coverages for individuals and families.

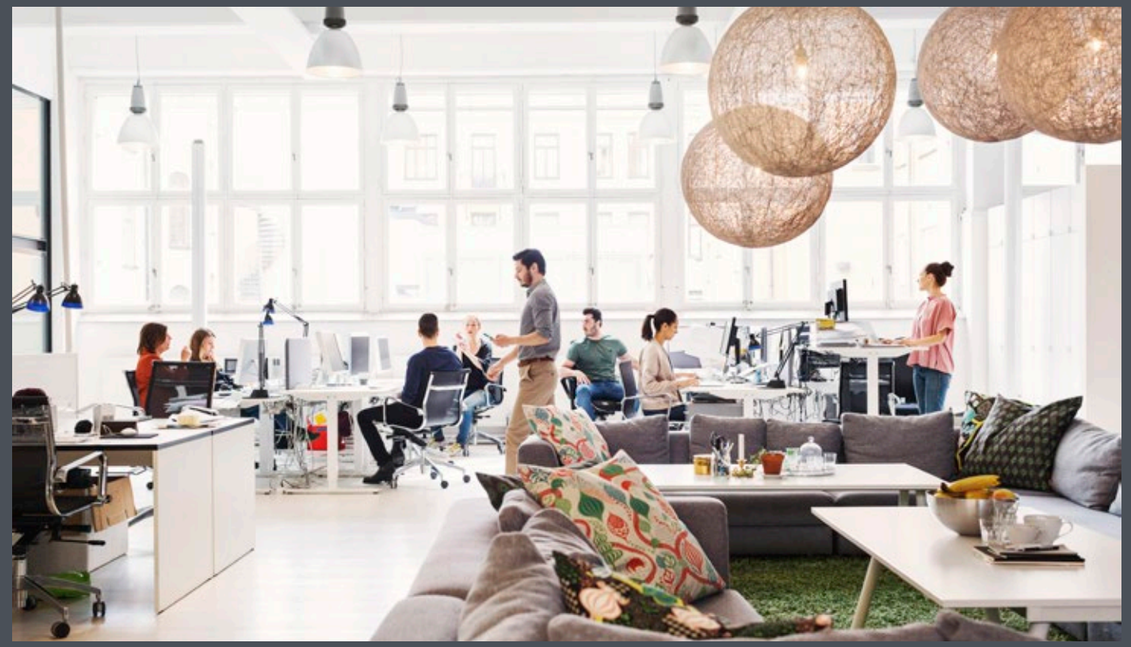
> "The new Chubb is now a superpower in the global P&C and A&H markets"

We not only help our customers protect themselves against the most basic kinds of risk but also the most complex and unexpected ones. We hold ourselves to exacting standards and we meticulously conceive and craft the best possible insurance coverage and service we are capable of delivering.

Olivier Reiz, Sales and Distribution Director for Continental Europe, says: "The combined risk appetites enable the new Chubb to develop some industry-specific expertise. Those 'industry verticals' will position Chubb as a one-stop shop for those sectors, which we know our middle market customers value. Current live examples include life sciences, new technologies, real estate, construction, fashion, luxury or entertainment.

"As part of our middle market strategy, more industry verticals will be developed in the future, as well as packaged products. That move was already initiated by each legacy company separately before the merger announcement, and will be accelerated going forward.

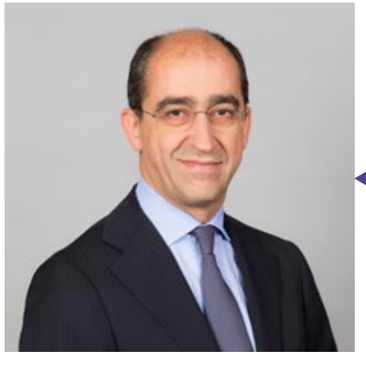
"The new Chubb is now a superpower in the global property and casualty (P&C) and accident and health (A&H) insurance markets. That positioning as a true global leader reinforces our multinational capabilities, as well as our engineering and claims servicing capabilities," says Olivier. ■



Photography: Getty

Stronger for our clients

People working for the new Chubb across Europe give us an inside view of the new company and explain why the acquisition has created a first-class insurer



New offerings

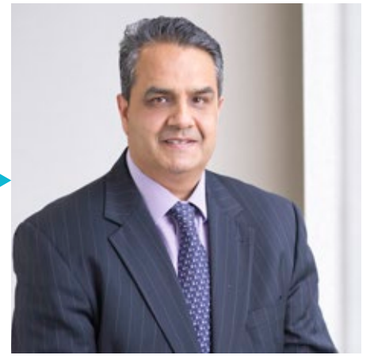
"We have clearly defined the business segments that we will have to best serve our customers - Global Accounts, Middle Market, Chubb Easy Solutions, High Net Worth Personal Lines, A&H and SPL - and we are excellently positioned in each."

Jeff Moghrabi
Division president, Continental Europe

Recognised by the industry

"Service is a key focus and we are proud to have won 'Insurer of the Year' at the UK Captive Services Awards. Chubb also received the UK Insurance Times Claims Excellence award for Insurer Claims Initiative of the Year - Commercial Lines."

Jalil Rehman
Executive vice president and chief business operations officer, Europe



Customer-centric

"Our approach as a new company hasn't changed, but it has strengthened: we are flexible, creative and customer-centric. The way we do business or deal with claims is all about offering excellent service to enable employers and their people to carry on 'business as usual'."

David Robinson
Executive vice president, Europe and president, UK and Ireland

Increased efficiency

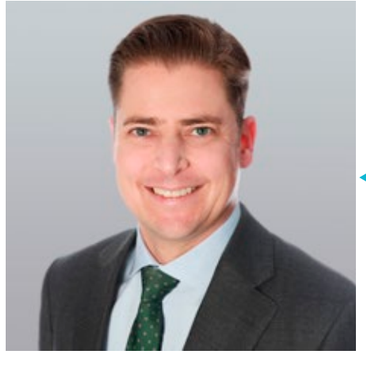
"In our market (Germany) we will be one of the top five carriers in some areas, such as professional lines, so our clients and brokers will have access to a broader network in underwriting and claims services, improving response times and product innovation."

Andreas Wania
Country president for Chubb's Germanics region

Awesome combination

"I believe that we make an awesome combination. The acquisition has brought together Chubb's 130 years of underwriting insights and devotion to customer service with ACE's three decades of technical underwriting excellence, broad risk appetite and global presence."

Nadia Côté,
Country president for Chubb in France



Even stronger

"ACE and Chubb, were very successful organisations in their own right. Together, we are even stronger. Brokers and clients benefit from a broad portfolio, the knowledge of experienced teams all across the organisation, a strong balance sheet, and a multinational footprint that is most likely second to none."

Florian Eisele
Country president for Chubb in Switzerland

Best of both worlds

"ACE brings an entrepreneurial spirit and innovation in products, services and distribution, as well as excellence in execution. Chubb is known for discipline, rigour and excellence in managing its processes, management information, claims and underwriting."

Olivier Reiz
Sales & distribution director for Continental Europe

Innovative solutions

"We are two organisations with people who know their crafts. Together, with our breadth and depth of industry knowledge, we can bring even more innovative solutions to the market, and we can do so at a speed that we know will shake up our competitors."

Eileen Castolene
Director of operations for Europe, Eurasia and Africa

Better products

"The synergies between the businesses are fantastic. When you put us together we're able to offer the best of both, whether that's our multinational offerings, niche/specialist items or our product wordings. Combined, we have better products."

Mark Roberts
Casualty manager for the UK and Ireland

Living in smart cities

Elinor Zuke considers some exciting developments in the cleantech sector and the risks that are involved

Our cities are reaching a crunch point. The UN predicts that the proportion of people living in urban locations will rise from 54% of the world's population in 2014 to 66% by 2050. For these billions of city-dwellers, resources are becoming scarcer and more expensive.

Technology is rising to the challenge, with cleantech companies big and small piling in to develop the kit that will both improve living standards and reduce energy consumption. Some estimates put the smart energy technologies market at US$220 billion worldwide by 2020. According to Bloomberg, worldwide investment in clean energy reached US$47.7 billion in the first quarter of 2014 alone.

"Cleantech is no passing, unprofitable fad," a report by management consultants McKinsey concludes. "The sources of underlying demand – a growing middle class around the world and resource constraints – aren't going away, and cleantech is pivotal in dealing with both."

Venturespring, a venture development firm that helps to incubate and accelerate new digital companies, sees an interest from some of the world's largest companies to invest. Managing director and co-founder Cassandra Harris says: "We've now seen everything from smart car technology to drones that can detect parking spots.

"The energy revolution will be driven by consumer needs and we are seeing more and more of this in the market now. The convergence between digital technology and the world of energy, or Energy 3.0, will pave the way for a new ecosystem of services which will enable both a better quality of life and reduced energy consumption."

Smart thinking

Meanwhile at home, the Internet of Things – which puts everyday objects online, allowing them to send and receive data – is a big area of development. For example, companies are fitting water meters controlled by smartphones that enable people to run their washing machine overnight when it costs less. Others are developing technology that fits on to a tap to disperse water more efficiently. Dutch energy provider Eneco offers Toon, a subsidised internet-connected thermostat, as part of its fixed energy tariff.

Every home in Britain, for example, will be fitted with a smart meter for gas and electricity by 2020. This will use a national communication network to automatically and wirelessly send energy usage information to the utility supplier. Smart meters will also come with a digital display to inform households about their daily energy usage and cost, encouraging a self-regulated reduction in consumption.

The technology is helping public infrastructure just as much as private homes. In Cambridge, where gridlocked roads are a common complaint, the city is planning to invest in smart technology that could change traffic light sequences at busy times ▶

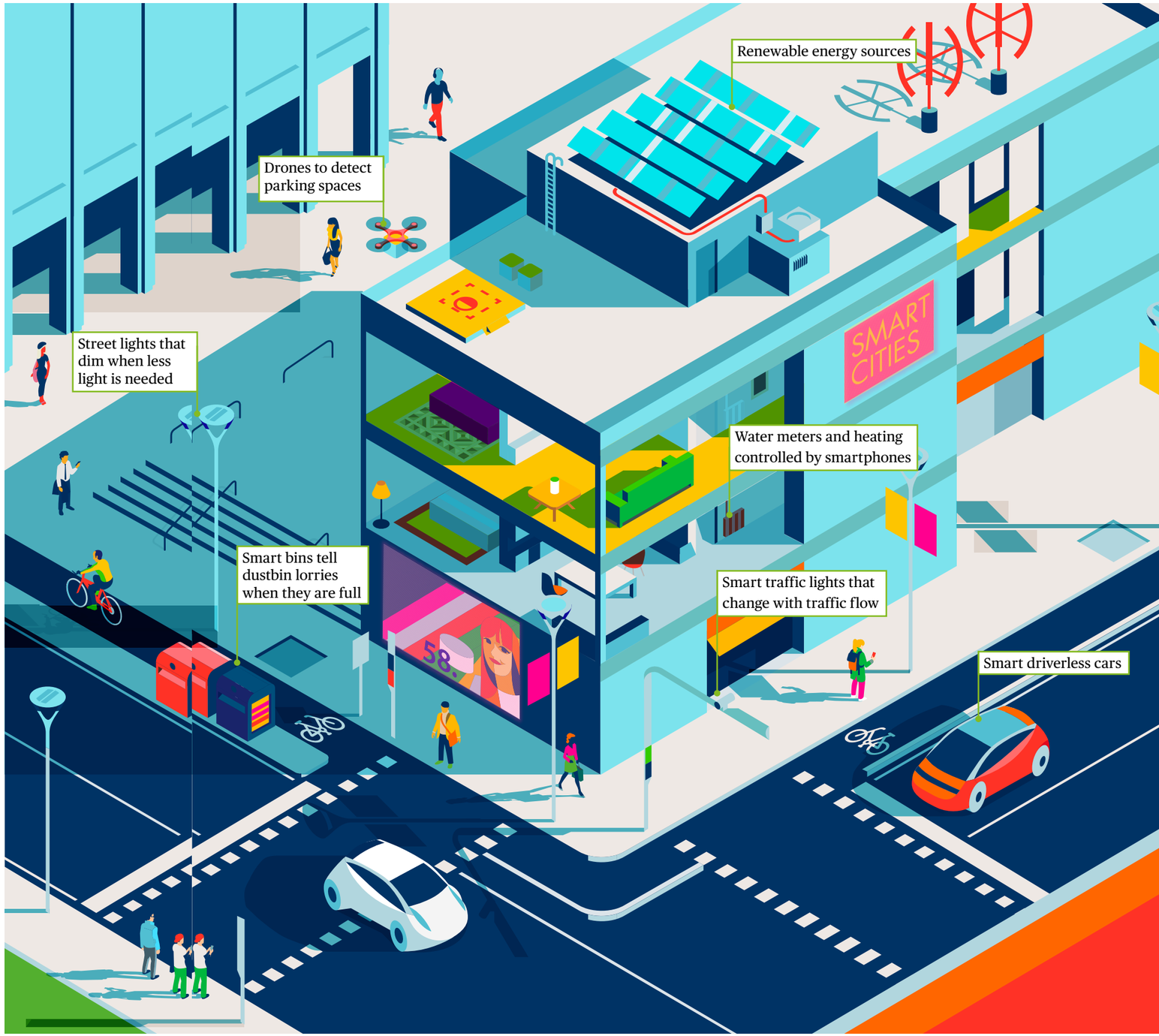


Illustration: Hey

by using a variety of real-time monitors to predict and control traffic.

This development, says Helen Troman, Head of Cleantech for Europe, Eurasia, Africa and Latin America at Chubb, reflects that cities are defined by how people live and behave. "The challenge faced by cities is how to motivate commuters to get out of their vehicles and take alternative, more efficient forms of transport, thereby reducing congestion," she says.

Some European cities have reduced their bill for street lighting by using LEDs and sensors that dim when less light is needed. It could go further. "Street lights could actually be incorporated into cleantech strategies. They could become platforms for a range of other sensors and could be used, for example, to collect data to support traffic management, or could even incorporate solar panels within their design," says Helen.

Other clean technology looks to minimise waste. US firm SmartBins fits municipal waste containers with wireless ultrasonic sensors that record and communicate how full the bins are.

Its software then creates routes for waste collectors so that only full bins are collected, with the routes sent directly to the drivers' tablets or smartphones. The technology, the company claims, can reduce service costs by up to 50% as well as reducing its carbon footprint.

Tech firms are also investing in solutions for areas without existing city infrastructures. Last July, Facebook revealed its first full-scale solar-powered drone, which it plans to use to provide internet access to developing parts of the world. Codenamed Aquila, the drone will be able to fly without landing for three months at a time and connect large rural areas to the net.

Some of these developments can have unintended consequences. An unexpected change in traffic light sequences on a familiar route could cause a car crash. A dimmed streetlight could lead to a rise in crime during the hours of darkness.

Data risk

But the biggest risk these technologies face is what makes them exciting and new - their use of data and online connection. "Personal information about the way you live your life is constantly available - and from an insurance standpoint, that's a concern," says Helen.

London firm Renew took a hit to its reputation when it was revealed that its 100 recycling bins in the City of London, which were fitted with digital advertising screens, were tracking the phones of passersby. It was ordered to turn off the technology and later fell into administration.

Top three takeouts for risk managers

1. **Build security into product development.** Security must be present from designing the concept, through the product's entire life cycle including patching or maintenance, and when it is decommissioned.
2. **Risk awareness.** Be aware of what data you have, where it is and the impact on your organisation if the data's confidentiality, integrity or availability is compromised. Understand the legislative requirements in all the territories in which you operate.
3. **Basic protection.** Detail procedures including roles and responsibilities at all levels and train your people to have security awareness. Encrypt all data at rest and in transmission and undertake network segmentation to protect sensitive data.

Firms will soon face financial penalties for data breaches under forthcoming EU Data Protection Regulation. "The new regulations will impose severe sanctions following a breach of up to €20 million or up to 4% of global group turnover, whichever is the greater, along with mandatory notification of individuals affected with all the associated costs," explains Andrew Russell, head of info tech, overseas general insurance for Chubb.

There is also a danger cyber criminals will hack into the reams of live data produced in the smart city. "Smart cities will pose an attractive target for cyber criminals. Imagine an extortion attack on local authorities or power companies threatening to take down power grids or crash traffic light systems, or simply attacks in the same vein by hacktivists for notoriety or terrorists for chaos," says Andrew.

The nightmare recently became reality in Western Ukraine when a cyber attack left 80,000 homes without power for several hours just before Christmas. Malware coded specifically to sabotage industrial systems successfully shut down the computers of one network and prevented them from rebooting.

British intelligence agency GCHQ has reportedly built extra security measures into smart meters after discovering loopholes in similar meters used in other countries, fearing that hackers could access the secure network to cut off the heat and light in British homes. The Department of Energy & Climate Change says it has put in place "robust security controls" and that only authorised parties will be able to operate the secure system that smart meters will operate on.

Lack of experience

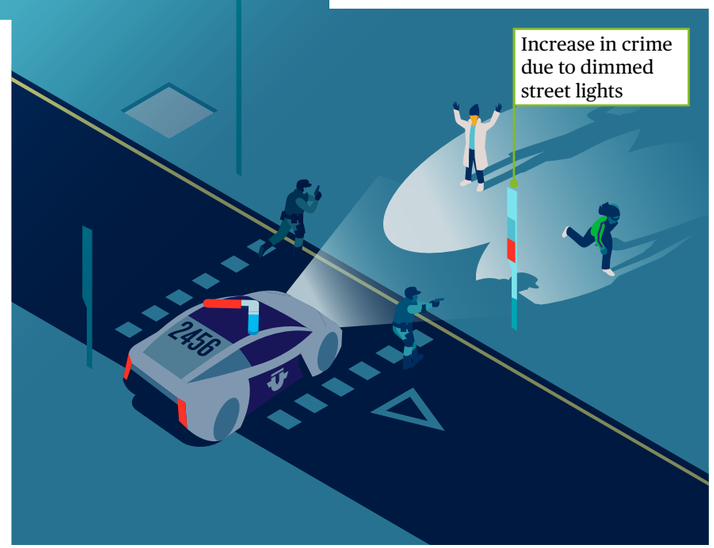
But Andrew warns that many companies developing new technology are leaving themselves exposed. "Many of these businesses will have little or no experience in the requirements of data protection or necessary technical controls. There are common instances of failure to incorporate appropriate controls or allow patching of software," he says.

Connected smoke alarms, which could send notifications to smartphones when homes are unoccupied, could be hacked into and turned off. Those challenges need to be addressed when new technology is in a pilot phase. "Many cleantech companies want to test their software in a live environment to prove its credibility," says Helen.

Cassandra advises start-ups to develop secure and reliable dedicated network infrastructures from the outset. "Network isolation ensures that breaches in one system do not directly lead to a breach in another system. Monitoring systems to detect and stop intrusions is just as important as securing the systems in the first place," she says.

When underwriting insurance for cleantech companies that host data, Chubb considers the credibility of the in-house team, how aware they are of their risk and what controls and practices they implement to mitigate those risks. "Our engineers work closely with cleantech companies and offer them risk management advice and guidance on best practice procedures. Clients also need to consider how regulation varies between countries," says Helen.

A survey of 300 cleantech CEOs conducted by Chubb, in collaboration with Cleantech Group, revealed establishing new partnerships, product-related R&D and global expansion as the top three priorities. The consequences of leaving data exposed could be fatal for even the best concepts. The winners will take every precaution to protect themselves from the start. ■



Get in touch

If you would like to discuss the issues raised in this article, please contact Helen Troman at HTroman@chubb.com

Cyber crime wave

Rob Brown talks to David Ralph, head of risk management and compliance at Hong Kong-based information and communications multinational PCCW

When a gang of elderly crooks tunnelled into a Hatton Garden safe deposit facility in London in April last year, they knew the risk. They also knew the potential reward: an estimated £200 million. But the rule of probability - the greater the reward; the greater the risk - caught up with them. Six men are now behind bars for the biggest heist in British history.

They'd have been better off online. "There's now less risk stealing money electronically than there is walking into a bank with a handgun," says David Ralph. And he'd know. As head of risk management and compliance at Hong Kong multinational PCCW, one of the territory's largest holders of personal data, it is his job to assess and mitigate the risk posed by cyber crooks. "The threat has increased significantly because there's so much money and much less risk involved for criminals."

So just how big is the threat? How does David manage it? And how are the risks he faces evolving? As troubleshooter at a multinational with a diverse array of interests, from telecommunications and media through to IT solutions and property development, what else keeps David awake at night? And how does he use insurance facilities to mitigate the risks PCCW faces?

Online crooks

In other words, the Hatton Garden crooks are dinosaurs. In the past year, cyber crime has jumped from the fourth most common economic crime to the second, according to a PwC survey of more than 6,000 global companies. It's the only crime that's growing, with more than a quarter of businesses questioned having fallen victim. Ominously, a further 18% are not sure whether they have been hit or not. Fifty companies reported losses to cyber criminals of more than US$5 million; the combined loss of a third of respondents was US$100 million.

The potential loot is huge. A 2014 McAfee report put global net losses to cyber criminals at US$400 billion. "Cyber risks are a significant concern for us," says David. "We've always been a technology company, so managing this has been a core part of our activities for many years. For companies that are just realising they now have a cyber risk, it would take up a greater proportion of time than it does for us. It's a case of making sure we're keeping abreast of what the emerging risks are."

The risks don't stop at PCCW's front door either. As the hacking of 15 million of a mobile provider's customers' personal details last year shows, crooks can gain access to sensitive data by manipulating a weak link at any point in a company's supply chain. In this case, crooks stole names, addresses and passport, social security and driving licence numbers by breaching the systems of data provider and credit agency Experian, which T-Mobile had used to run credit checks on its customers.

"There's always going to be a risk that vendors or even customers that you are allowing to connect to your systems for whatever purposes are not going to have adequate levels of security," says David. "We put in place a requirement that third parties maintain a certain level of security before connection is allowed. And if they are breached, we make sure we stop them at our doors rather than within their environment."

6,000
companies were surveyed and showed the extent of cyber crime

18%
of companies surveyed don't know if they have been victims

Internet of Things

As well as providing traditional fixed line, international data and mobile services through its telecommunications arm, PCCW also runs Hong Kong's largest pay TV service, a role that includes media production. The company is the territory's largest systems integrator, with data centres in Hong Kong and greater China. PCCW also has a burgeoning property development business. As the company has diversified, the risks it faces have multiplied. ▶

Photography: Jasper James

"What this Internet of Things does is increase the number of potential robots that could be used to attack an organisation"

A life of risk

- "I started doing information security in the early 80s before anyone understood what it was; people used to ask whether I had to carry a gun," recalls David, who joined what was then Cable & Wireless HKT in 1992 on a short-term contract to introduce a robust information security system as a new computer system was installed.
- By the mid 90s, David had become a full-time employee, overseeing an increasing array of risk management roles. "In 1995 or 1996 we outsourced a large part of our information systems to a major vendor and I was involved in looking at the outsourcing process, the various risks and contracts and things," says David. "My role became more holistic."
- "The real sea-change came in late 1999, just before Cable & Wireless HKT was sold to what was then Pacific Century CyberWorks," recalls David. "Once we were acquired locally we needed to have a more localised responsibility for the insurance (previously it had been managed in London). It fell to me to pick up much broader responsibilities across the company. By necessity I became a risk manager as opposed to a technology/security type person."
- The ongoing development of Tap & Go (see main story) is enabling David to further widen his skills. "This is actually a highlight of my career," he says. "I'm leading the licensing initiative. We have a fantastic team developing the product itself and getting it into the market - my responsibility is to work with the regulator to ensure that we get our licence as soon as practicable. We have a very strong desire to be the first one to be granted a licence, which creates its own set of challenges and opportunities as both we and the regulators are coming to grips with this new regime at the same time."

Of course, PCCW's growing property business, specialising in high-end apartments and resorts, poses the usual range of risks any business in the field faces. The telecommunications part of the business is also working with property developers and renovators, which raises different concerns around liability. "One of our services that's been very successful has been our Smart Living initiative, where we go into somebody's house and put in networks enabling smart devices to talk to each other on the internal networks as well as the internet," explains David.

"This is what we mean when we talk about the 'Internet of Things'. You can use your phone to unlock the door and at the same time open your curtains, your lights will come on, your TV will go to a certain channel and the coffee machine will turn on. We're putting these things into premises. Where the risk comes for us is the activity of installing them. Sitting behind that are manufacturers' liabilities that get passed on but it could be a problem for us in terms of reputation and vicarious liability."

That's not all: the greater the number of devices connected to the internet, the greater the risk of cyber attack. "It's a long way off before my fridge decides to hack my TV," says David. "But what this Internet of Things does is increase the number of potential robots that could be used to attack an organisation. The fridge actually could be used to initiate an attack against your Domain Name System service for example, as things go forward."

A lot to lose

David sums up the scale of the risk succinctly: "We could lose our reputation; everything. Our customer databases are the largest in Hong Kong outside of the government, so there's a lot of information that could cause us a lot of pain. Within personal data privacy ordinance we have the usual obligations to protect personal data, and in addition, we have specific privacy obligations under our telecommunications licences, so if the telecommunications regulator took umbrage with a breach, there's the potential of our licence being withdrawn or severely impaired."

This reflects a crucial and growing part of David's role: regulatory compliance. "This area has just continued to grow in my day-to-day role," he says, pointing to PCCW'S development of Tap & Go, a stored value mobile money facility. The company's first steps into the financial sector bring with them a number of new regulatory challenges.

$400bn
Global net losses at the hands of cyber criminals

50
The number of companies that reported losses of over $5m

"We're in the process of applying for a new type of licence issued by the Hong Kong Monetary Authority. In November, an ordinance was passed requiring stored value facilities to become licensed. It brings into play things like anti-money laundering, which is not really something that's been a traditional concern for telcos or any of the businesses that we were in before. It's a challenge, but obviously we went into this with our eyes wide open."

With PCCW's interests spreading further across the world (the bulk of its offshore business is acting as a carrier to multinationals or wholesaling to fellow telcos) increasingly David has to keep his eyes on the regulatory and criminal risks of each market. "We need to be aware of the regulatory environments we operate in; requirements may change at any given time," he says. "We're dealing with large multinationals and have commercially sensitive information for those companies, so obviously we have to be aware of the higher value of that to someone with nefarious intent."

The company uses a range of insurance facilities to mitigate such risks. "Our relationship with Chubb is very important," says David. "Most of the policies we have with Chubb are covering worldwide risks, more in the line of property liability, marine risks, professional indemnities, crime and so on. It's a relationship that we endeavour to maintain and expand as much as possible."

With technological advances continuing at such a blistering rate, the opportunities for companies such as PCCW are growing exponentially. But so are the opportunities for cyber crooks and therefore the risks for such companies. But David says: "The company has taken to heart the risk manager's mantra that risk is not all downside. There's opportunity in risk." So long as David continues to manage it. ■

Power to the people

Renewable energy is a continually fast-growing industry sector bringing huge benefits, but also its own risks, says **Andrew Pring**

The global renewable energy (RE) market has grown strongly in the past decade, with Europe among the leaders. Blessed with excellent renewable supplies from wind, water and even sunshine, the British Isles alone attracted over £12 billion worth of investment into the RE sector last year, for example.

While there is currently some nervousness among RE operators over government policy and the future of subsidies, it seems inconceivable the sector will not continue to grow in importance in Europe.

It's certainly a booming sector for some insurance specialists, which have been quick to adapt and find ways to help RE operators and investors manage their risk exposure in the newer embryonic industries through a range of innovative, tailored policies.

Risks of renewables

Ironically, for a form of energy that is environmentally friendly, some sectors of RE projects carry potential environmental risks, both during their construction stage and during operational life. Construction of onshore and offshore wind farms is carried out in coastal areas or pristine countryside. Through the creation of access roads with heavy vehicle usage and offshore vessel activity the potential is there to pollute surrounding fields, rivers and the sea through leakages and spillages, as well as to cause much harm to local biodiversity and protected species. The same problems can occur if equipment and infrastructure are not run or maintained properly throughout their lifetime, with leaking hydraulic fluid being a potential risk.

It's not just operations and power supply that are affected when things go wrong. Any ensuing environmental despoliation following a polluting loss can result in seriously punitive fines of hundreds of thousands of pounds – which, naturally, cannot be insured against in the way normal accidents are – in addition to the months of lost income while a plant is being repaired. Damaged land also has to be restored to its pre-existing state, which carries a cost.

Traditional insurance was found to be inadequate for environmental liabilities so a new market has sprung up since 2000, which covers all eventualities across the pollutant and environmental risk spectrum.

Emma Bartolo, Chubb's UK & Ireland environmental risk manager, says the company has been writing renewable energy insurance policies for well over a decade across the world and is particularly active in the UK at the moment. As well as the risks outlined above, she says, there are other environmental risks that need to be considered with RE projects.

These include air emissions such as dust created during construction and sediment leaking into rivers or the water table. Fire is another relatively common risk, as are hydraulic oil spillages from wind turbines. And escaping odours from anaerobic plants have led to class actions from legal residents against what is officially described as "nuisance".

Anaerobic digestion (AD), which produces biogas that can be used as fuel in combined heat and power gas engines, has become a big growth area for Chubb. There are over 350 such plants in the UK and the technology is well established, but accidents occur quite frequently. "One example," says Emma, "was at an anaerobic plant that was part of an agricultural university in South Wales. It was using waste for energy from local farming practices but a bolt in one of the tanks failed ▶

Photography: Getty

and the tank burst, leaking the waste onto nearby land and into streams.

"They were covered by their policy and we paid out £260,000 for the clean-up. But they also suffered £250,000 in business interruption costs, as the university relied on the plant for energy and had to close. They weren't covered for that because the insured opted not to purchase the business interruption extension offered when they took out the policy.

"Six months later, at the same college, an operator left a pump going overnight and the tank exploded. This time it cost £350,000 for clean-up, and by then they had cover for business interruption costs of a further quarter of a million pounds."

Improving technology

Working with RE clients to ensure they have the best insurance cover against risks such as this is one of the services provided by JLT Specialty. Part of Jardine Lloyd Thompson Group, JLT Specialty has placed the insurance for over US$150 billion of energy construction project values (onshore and offshore) over the past six years, as it seeks to help clients improve both the insurability and bankability of their RE projects.

Duncan Gordon, an associate in JLT Specialty's Renewable Energy Practice, says the RE insurance market has matured considerably in the past decade. "Some risks are certainly being viewed quite differently to a few years ago. There are increasingly more insurers coming into the space. The technology is improving, especially in wind and solar, so certain mechanical failures are reduced with a good maintenance programme and the abundance of projects and improved experience drive down costs.

"As a result, operators build a track record and a loss and claims history, so the risk profile has improved and there's much more confidence amongst insurers in certain sectors." AD plants are a busy area for JLT Specialty. JLT's clients predominantly fall into two groups - investment funds that are bankrolling a number of plants contained in portfolios and developers who see an opportunity to offer energy, typically through a one-off AD plant.

> "Technology is improving, especially in wind and solar"

Maturing market

Maintenance and operations training of AD plants is a key risk, says Duncan. "In some instances, once the plant is built, the contractor moves on after training the ongoing operator, who is left responsible for the plant. Things can go wrong unless they are monitored and operated efficiently, and some of the major failures can cause collateral environmental damage in addition to the material damage costs and lost revenues.

"So the first thing we would discuss with project owners looking to go down this route is to ensure the operations training is in-depth and there is a planned maintenance agreement in place. We'd also look at what experience the operator has, and their relief and ongoing training arrangements with the contractor/installer. These are just a few of the key aspects from the project risk matrix which insurers would expect to see."

Duncan adds: "If a project causes pollutant contamination of the surrounding land, standard third party and pollution liability policies are only triggered if the loss causes third party damage by sudden occurrence of the pollutant. More innovative policies can pick up this pollution damage and clear up costs even if it occurred gradually over time.

"This is an important attribute as the cover can respond to an order to restore the land following a pollution event. It can also cover the associated revenue lost during this period of clean-up and restoration." ■

Top three takeouts for risk

- Work with brokers and insurers that have specialist RE teams and an extensive network of RE advisers. In such a relatively new market, companies with experience and invaluable insights across the entire risk spectrum will deliver the best deals.
- Look for a bespoke, matrix-based approach to providing insurance cover, rather than relying on standard policies. This will help meet all contractual requirements, and could increase a project's bankability.
- RE projects are often vulnerable to operational failure, which can have an impact on the businesses to which they're supplying energy. Business interruption insurance is always worth including in the coverage package.

Get in touch

If you'd like to discuss any of the issues raised in this article, please contact Emma Bartolo at Emma.Bartolo@chubb.com

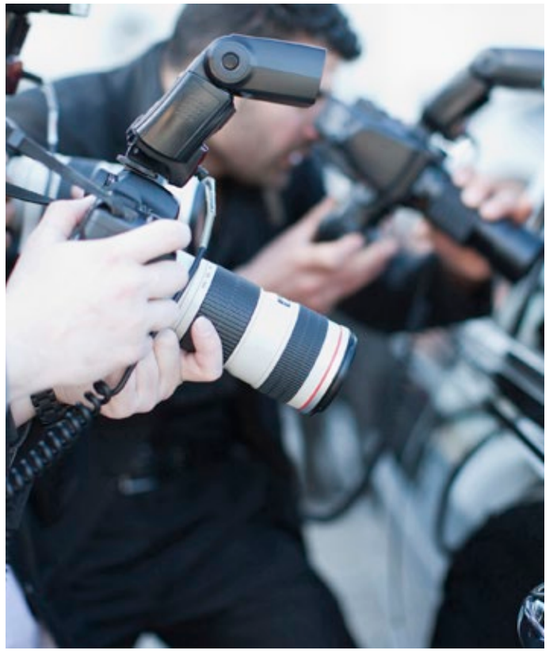
Cyber scares

Simon Creasey finds out the real cost of cyber attacks and IT outages, and how companies can minimise the risks

It was the news feared in boardrooms everywhere - cyber criminals had compromised the systems of a major European company and stolen sensitive data. The incident happened in the morning, and by the afternoon, the insurance industry knew what was going on. By the evening, the cyber breach had become headline news globally, with significant potential implications for the business's reputation and brand.

In the wake of the attack, the business was criticised for not knowing the extent of the breach (which was not nearly as bad as had initially been feared); for the lack of information issued to its customers; and because it had been compromised previously. ►

Photography: Pixeleyes



According to business continuity experts, when managing interruption incidents of this nature the general objective is to ensure they remain just an event and not a headline. So how can companies that are victims of an IT outage or, even worse, a cyber attack, ensure they don't become headline news? And if they are subject to an attack, what can they do to ensure the income loss to the business is minimised?

Attacks on the rise

Over the past decade the number of cyber attacks on businesses has grown significantly and, despite the best efforts of many business owners, a number of attacks have been successful. Over the same period, demand for cyber risk policies that include business interruption insurance to cover business income losses has risen so that companies can offset any losses.

But according to Paul Handy, head of global technical services for Europe and operational head of cyber risks at Crawford & Company, establishing the financial loss to a business isn't a straightforward process, particularly as no two claims are the same. He breaks the nature of incidents into two areas: cyber attacks on, or losses stemming from an outage to, IT equipment or systems that are owned by the insured; and interruption or losses caused by the same set of circumstances at a service provider.

The more straightforward loss to establish is when, as a result of a hack or an 'event', a business's systems are impacted or shut down. "There is a direct or tangible link between the attack and the insured's ability to trade and therefore you can quite easily calculate the resultant business income loss," says Paul.

Where it becomes slightly more complex is when a cyber event occurs that impacts on the brand or reputation of the business that may affect a company's income stream because people no longer want, or are less inclined, to do business with that company.

"That's a more complex calculation to do," says Paul. "It's not clear, it's less tangible and more subjective. What we have to do is look at historical revenue streams and we build into that seasonality, trends and other circumstances that might impact revenue streams. Then we project that forward to determine what the business would have accrued, but for the incident. That enables us to calculate, or estimate, what the losses to the business might be."

The other main element of business income loss is "dependent income loss", which occurs when a service provider – for instance, a company that supplies a cloud database or offsite server – has an IT incident that results in lost revenue for its customers.

"You can control what happens and how you manage your own systems, but when it comes to your service providers, it's one step removed and underwriters perceive this to be a major risk," says Paul.

"There is a direct or tangible link between the attack and the insured's ability to trade"

Photography: iStock

"They're realising that they have to invest more heavily in intrusion detection and prevention software"

Ready for anything

While companies might not be able to control issues that occur at their service providers, what they can control is how they deal with these issues as and when they arise. How a company responds in the early hours of an incident can have a major impact on the extent of the losses, says Paul.

"These are brand-threatening events so the first 48 hours are critical in order to protect the business," he explains. "If you sit on the problem these events can be catastrophic and the decisions you make at the early stage of a claim can have a massive impact on potential revenue losses."

He adds that the earlier businesses such as his are called in to assist, the better the outcome. "We deal with many incidents where we get involved very early on and work with the insured to understand the nature of, and help them to respond to, any potential breach, bringing in our specialists when required," says Paul. "We help manage the regulatory notification process in line with what are often differing or multi-jurisdictional guidelines and requirements.

"Coupled with the regulatory process, there is a need to carefully manage customer messaging and PR. Without dismissing the gravitas of a breach event and the potential impact on the individuals concerned, the approach adopted by a company in notifying and supporting their customers can have a direct impact on the propensity for litigation and, importantly, reduce the potential for negative publicity and the resultant detrimental impact on the business. Our experience is that, if these events are managed well, they needn't have an impact on the business and can often fall away long before any claims or negative headlines are made against the organisation."

Planning ahead

Pre-event planning is another way companies can offset the impacts if the worst-case scenario occurs.

"There is an absolute correlation between those businesses that are event ready and those that are not," says Paul. "The results and the potential losses are greatly reduced at those companies that are event ready compared with those businesses that, when something happens, start scratching their heads."

The good news is a growing number of businesses have already started to put in place some of the necessary measures to make themselves event ready, says Paul. It's a view shared by Tim Stapleton, vice president, cyber insurance product manager, overseas general insurance at Chubb, who says that there has been an evolution in the way companies approach the area of business interruption.

"We're starting to see a shift from front end defence systems to the back end," says Tim. "So they're looking at things like how quickly can we identify and remediate an issue like this? Firewalls, penetration testing, password protection – those are all front-end defence measures that companies use as a baseline, but we're beyond that stage now. They're realising that they need to invest more heavily in intrusion detection and prevention software and they need to invest heavily in encryption."

This is just a taste of some of the wide range of different measures that companies are increasingly considering, according to Tim. "Others include how often do they back up data, can they switch to another server if they need to shut one down that's been attacked, do they have a robust business continuity plan in place, do they have disaster recovery planning and how quickly could they bounce back from an event? Those are controls that companies are shifting towards," he explains.

Cyber crime is a growing industry and it's clear that the threat isn't going to go away any time soon. Businesses that embrace these safeguards, together with the other measures outlined by Paul, are putting themselves in a strong position to react to an event when it does occur.

"There is a consistent way we deal with these events or claims. By applying a considered or project-managed approach to the event circumstances, it helps to reduce the risk and any corresponding or potential impact on the business," says Paul. "By reducing the risk, you are immediately helping the business steer and manage itself out of that crisis."

This ensures an event stays just that – an event and not a headline on the evening news. ■

Five tips

1. Don't be complacent: no one is immune from IT outages or cyber attacks – governments, public bodies and private companies have all suffered from cyber-related incidents in recent years.
2. Always remember, the key to minimising the financial impact of these incidents is how you respond to the attacks.
3. Pre-event planning is vital – companies need to work out an instant response strategy for dealing with incidents and these plans need to be tested on a regular basis.
4. When an incident occurs, in addition to triggering the instant response plan, it's also important that companies notify their insurance provider as soon as possible, because the decisions made at an early stage can have a significant impact on potential revenue loss.
5. Above all, the first 48 hours of any IT event are critical and a good insurance provider can advise companies on how to minimise their losses.

A passion for power

Collecting classic cars is more than just a hobby for some high-net-worth investors

It is perhaps unsurprising that high net worth individuals tend to own valuable and unusual cars, but for many, a passion for collectible motors has also turned out to be an extremely shrewd investment.

Investments in classic cars saw annual growth of 17% globally, the top-performing investment of passion, according to figures from the Historic Automobile Group International and Knight Frank. Over the past decade classic cars have increased in value by 490%.

Some individuals own as many as 250 cars, with the largest collections worth in excess of US$200 million, according to Matthew Pearce, European motor manager at Chubb. Historic Ferraris have led the pack: in 2014, a 1962 Ferrari 250 GTO sold for US$38 million – the highest price yet paid for a classic car at auction.

Although most car collections are kept in museums or in specialist storage, they are also driven and taken to concourse events or raced in heritage rallies, sometimes on the other side of the world.

Collectible cars are most akin to fine art, and damage to a vehicle – even if expertly repaired – can result in depreciation.

Matthew says: “Insurance will pay the cost of repair should a car sustain damage, but uniquely, Chubb will also cover any resulting loss of value.” ■

Photography: Getty

Insuring the super rich

From Ferraris to high-end Swiss watches, wealthy people are demonstrating a passion for unusual and high-value assets, with big implications for their insurance protection, writes **Stuart Collins**

Despite a bumpy ride for the global economy and a slump in commodity prices over the past ten years, the rich have nevertheless grown both in numbers and in wealth.

The past decade has seen a 60% global increase in ultra high net worth individuals,* with around 187,500 people accounting for some US$20 trillion in assets, according to property consultant Knight Frank. Lower down the wealth scale, there are also estimated to be around 13 million high net worth individuals, with a combined wealth of US$66 trillion. That's similar to the value of global equity markets.

While many people may associate wealth with fame and notoriety, high net worth individuals do, in fact, come in all shapes and sizes.

Most are just very successful in their chosen field, be it business, sports or entertainment, according to Tara Parchment, personal risk services manager for UK and Ireland at Chubb. Tara says that, in contrast to celebrity culture, many are accustomed to their wealth and are proactive in managing their risks and lifestyle.

Risks of wealth

While there is no typical profile of a high net worth individual, there are some common risk characteristics. The lifestyles and assets of wealthy people are often high value, complex and global, explains Tara.

"High net worth individuals will typically own multiple properties, and will move valuable personal possessions from one home to another. They will also have high-value physical assets and investments, ranging from super-yachts to collections of fine wines."

London and New York are the most favoured locations for these wealthy individuals, with the UK capital boasting the highest concentration of rich people in the world.

But wealthy people tend to be highly mobile, travelling between homes and sporting, art and business events.

According to a study of private jet usage by Knight Frank in the UK, a typical year will see some of these people ski in Davos in January, attend the Masters at Augusta in April and the Monaco Grand Prix in May, before ending the year at Art Basel in Miami.

A notable trend in recent years has been a shift in investments from the financial market to physical assets. These include so-called passion investments, such as classic cars, fine art, jewellery or investment-grade Bordeaux wines. Over the past 10 years, fine wine values have increased by 241%, second only to classic cars, whose prices have rocketed by a staggering 490%.

Top prices also continue to be paid for fine art and jewellery. Last year, Paul Gauguin's painting of two Tahitian girls, *Nafea Faa Ipoipo*, broke records when it achieved nearly US$300 million at auction, while a new record price of £40 million was set for a rare blue diamond in May 2016.

Rising demand

The shift to physical assets and investments of passion has resulted in increased demand for insurance, reflected in the growth of the high net worth insurance market. ▶

"Specialist high net worth insurance has never been as important"

Given the high values of high net worth assets, specialist high net worth insurance has never been as important, according to Christopher Tully, managing director of the insurance broker and Chubb agent Symmetry Private Insurance. "The wealthy are getting wealthier and the value of many assets has never been so high, so there is a lot more to lose," he says.

Whether it is fine wine or fine art, it is critical to understand the nature of the asset, how it is stored, and its value, explains Tara. "These are possessions that their owners are passionate about," she says.

One of the biggest challenges for high net worth clients is to get the sums insured right. Christopher advises: "Always put in the effort when arranging insurance to verify the sums insured, and make sure that they reflect the value of assets."

Christopher was recently approached by an individual who had not had their jewellery valued since the 1990s. The value of gold and diamonds has more than doubled over the past 20 or so years, he explains.

As physical assets have increased in value, and as lifestyles have become more complex, getting the right advice and insurance cover has become crucial, according to James Wasdell, director and co-founder of the insurance broker and Chubb agent Quantum Underwriting Solutions.

Many high net worth individuals either arrange their own insurance directly or delegate it to others. Too often the result is inappropriate insurance, underinsurance or worse, he says.

James recalls one wealthy individual whose personal assistant purchased insurance for one of his properties using a comparison website. Unfortunately, a valuable item was later damaged in a burglary and was not covered by the off-the-shelf policy.

"It can seem intrusive, but the key is to understand an individual's wealth. Once you drill down, you really see the complexity of their assets and liabilities," adds James.

The right insurance

While specialist high net worth insurance is a must, not all insurers in this market are the same. Christopher has been a high net worth insurance broker for more than 30 years. He says policies differ in the exclusions and conditions they contain, with some insurers limiting certain coverages.

High net worth clients will want insurance that does not impinge on their lifestyle. Insurers may request that high-value objects, such as watches and jewellery, are placed in a bank vault when not being used. Christopher says: "The high net worth market will place conditions on policies, but insurers like Chubb will work to remove them."

Tara says that a good underwriter will put a lot of time and effort into understanding their client's lifestyle, as well as their property and possessions.

She says: "We usually meet with clients and visit their properties, appraising their risks and agreeing values upfront. The aim is to ensure that in the event of a loss there are no grey areas."

Insurance is not just about protecting valuable assets, Tara believes. It's about lifestyles too. She says that, for example, Chubb offers family protection cover to pay for expenses such as counselling following a burglary or carjacking.

It is even possible to insure against cyber bullying or identity theft, and the insurance will pay for investigations.

She adds: "We look at all the risks impacting high net worth individuals and look to guard against them, whether it's a classic car collection, the family home, the risks of legal action or cover against cyber bullying."

High net worth insurance is not just about the traditional perils of fire, theft and water damage, explains Christopher.

"There is so much more that can impact the lives of high net worth individuals. New insurance benefits, such as cyber crime and family protection, are becoming more relevant," he suggests. ■

*Ultra high net worth individuals are defined as those with US$30 million or more in net assets, excluding their principal residence

Held hostage

Kidnapping is big business across the world, but companies can manage the risk with smart planning, writes **Liz Bury**

Photography: Pixeleyes

Kidnapping is a global threat, and usually involves a financial ransom demand by criminal gangs, drug cartels and sometimes even corrupt police. Although some victims are taken by religious or political extremists with ideological motivations, the payment of a ransom is usually required to free a hostage.

In the Western Hemisphere, Mexico is currently the "kidnap capital of the world", with literally thousands of cases every year. Venezuela comes a very close second. Meanwhile hundreds of cases are reported every year in Honduras, El Salvador, Colombia, Brazil and Argentina.

In Africa, kidnapping is a critical problem in the Sahel, and has grown exponentially in parts of Nigeria, Sudan, Kenya and Somalia. The Middle East, Afghanistan and Pakistan are all high-risk areas. Kidnapping can also be an issue in countries such as India, Indonesia and the Philippines. ►

“Every kidnapping victim has a market value. It sounds crude but that’s how it is”

Wesley Odom is a former CIA operative and president of The Ackerman Group, a specialist crisis response agency that has negotiated the safe return of hundreds of kidnap victims.

Wesley explains that kidnappers almost always have a “type” of target they focus on, with certain people much more likely to fall victim to this terrifying crime.

Who’s at risk?

“The most frequent targets of a kidnapping for ransom are local nationals who work for multinational companies, often the country manager or plant manager,” he says. “Often they are targeted not for their affiliation with a multinational company, but because they are perceived to be affluent.

“They tend to live in a nice home in the best part of town, and as such they look like a good target. In some cases, it was the child of the executive who was snatched, so we had to negotiate their release. While all cases are nervewracking, when a child is involved it’s particularly so, and something no family or corporation wants to go through.”

In some territories, new methods of kidnap are starting to emerge. One that is increasingly popular among criminals is ‘express’ kidnappings.

“This is happening all over the world, but particularly in Latin America. It’s a crime of opportunity,” Wesley explains. “Anyone, from the wealthy local resident to the business traveller or tourist, could be a target. For instance, the victim may simply get into the wrong taxi in Mexico. The driver stops and picks up a couple of confederates and they take you at gunpoint to an ATM machine to take out money.

Photography: Getty

300
The number of kidnaps dealt with by Ackerman

0.5%
of ransom payments are to proscribed organisations

“They may even hold you past midnight, take you to another machine and get the next day’s limit and finally kick you out of the cab. If you are lucky, you’ve lost several hundred dollars and you’ve been kidnapped for only four or five hours.”

Also on the rise are ‘virtual’ kidnappings, where a gang contacts an individual or family and convinces them that they are about to be kidnapped or that someone in their family already has been. A ransom is paid by the victim, who only discovers later that no one was actually kidnapped, or even at risk.

Securing a release

The majority of kidnap gangs are criminals, be they local thugs or more sophisticated, organised syndicates. All approach kidnapping purely as a business transaction.

Neil McCarthy, management liability manager for UK and Ireland at Chubb, says that every kidnap victim has a market value. “It sounds crude, but that is how it is. There is a recognised market value for the victim, depending on who takes them, and that informs the negotiation strategy you employ to get the person back.

“Chubb offers a kidnap, ransom and extortion policy that covers organisations and businesses whose personnel may become kidnap targets. We have a preferred supplier arrangement with Ackerman, so in the event of a kidnapping, the agency will fly out a consultant to the territory in question to support the family and handle negotiations.”

Wesley explains that with nearly 40 years of experience in this field, Ackerman has a tried and tested methodology for managing negotiations with kidnappers. Once a settlement is agreed, Ackerman will safeguard the money and arrange for the delivery of the ransom. Then it’s largely a waiting game. “You have to wait until the kidnappers release the hostage(s). There is rarely a simultaneous exchange of ransom for hostages,” he says.

David McFadyen, crisis management practice leader at brokers Aon Sweden, says: “To trigger the kidnapping coverage on a policy you need a kidnap for ransom, and beyond this there are two major expenses: the ransom itself and the crisis management response. If you have a crisis management consultant on board for the duration, and it turns into a long, drawn-out negotiation, that can be an enormous cost.

“There’s no average ransom. It depends where you are and how sophisticated the kidnappers are. It’s a long, complicated process and it’s important to not just pay what the kidnappers want, because that can lead to a situation where the kidnappers might realise the client has an insurance policy and try to reopen negotiations.

“The consultants understand the intricacies of these situations. It’s absolutely critical that the negotiation process is handled correctly.”

Ransom demands

In the UK, the Terrorism Act 2015 has made it illegal to pay ransoms to UN-proscribed organisations, including Al Qa’ida, Al Shabaab and ISIL. However, as Neil says, this doesn’t prevent Chubb’s policy from paying for expenses. A significant part of any kidnap or extortion event loss costs is the negotiators’ fee and associated expenses.

“The Act only prohibits payments to a UN list of organisations known to exist for the purposes of terrorism. In the past ten years, fewer than 0.5% of ransom payments have been to proscribed organisations.”

A critical element of the cover is confidentiality, David at Aon Sweden explains: “We have to make sure that the knowledge of such insurance is restricted. A process should be implemented so that ▶

“There is no average ransom. It depends on how sophisticated the kidnappers are”

In some countries, simply getting into the wrong taxi could be the beginning of a terrifying kidnap ordeal

people in the organisation, especially those in risk management, understand - maybe not that there's an insurance policy in place, because only a few people at a high level know about the policy - but that there is a preferred response firm they should use."

Hard targets

Wesley at Ackerman says that kidnap prevention training focuses heavily on behaviour modification rather than armed executive protection, although there is a time and place for the latter. "In our experience, the kidnap gangs will often identify two or three executives as potential targets and then zero in on the one who predictably leaves his house every day at 07.00 on the dot, drives the same route in the same car, eats at the same restaurant every day and so on.

"But if the guy sometimes leaves his house at 06.00, sometimes at 08.00, drives a couple of different vehicles and takes different routes, then he's a hard target. We teach executives to modify their behaviour by being unpredictable."

Rates are soft for kidnap and ransom insurance right now, and those interested in buying can expect to get a good price.

David at Aon Sweden says: "Policies include the response services of an expert crisis management company, and in some cases the insurance is cheaper than if you were to approach one of those crisis management companies separately and pay them a retainer to be on standby in case."

Many policies cover loss of income, a range of expenses, psychological treatment after the event, material losses and political evacuation - something that has been triggered a lot in recent years, Neil at Chubb says.

"If you look at what happened during the Arab Spring in places like Egypt and Tunisia, people had to get home and get home immediately. You've got to get out however you can - charter a flight or a helicopter in some cases - because it's an emergency."

Out of almost 300 kidnap situations, Ackerman has lost only three hostages. In one case, the victim had a heart attack while being held, and in another the body of the victim - who was wounded during the abduction and for whom proof of life was not provided by the kidnappers - was never recovered.

A third man was very unlucky. Wesley explains: "We were working with the highest levels of the national police, but unbeknownst to all of us, a precinct-level police crew acted on an anonymous tip and raided an apartment complex. It turned out to be the safe house where the victim was being held. The kidnappers shot him as the police burst in.

"We've never rescued a hostage, nor would we advocate doing so. In most cases, the most dangerous thing you can do to a hostage is to attempt a rescue operation." ■

Get in touch

If you would like to discuss any of the issues raised in this article, please contact Neil McCarthy at NMccarthy@chubb.com

Focus points

Prevention techniques

Make yourself and your staff a hard target. Abducting an individual is difficult and the criminal gangs who perpetrate kidnap for ransom will pick an easy target. Practising kidnap prevention techniques, such as varying daily routines, can discourage kidnappers.

Potential targets

The most likely victims of kidnap for ransom are local nationals, particularly multinational executives and expatriates living abroad for work. Business travellers have a low risk of becoming a kidnap victim. Those who are visiting a kidnap-prone country for a short stay generally only become victims of kidnap if they happen to be in the wrong place at the wrong time, with someone who is the target.

Ransom negotiations

Ransoms vary depending on geography, the level of sophistication of the kidnappers, and who the victim is. Expert negotiators are best placed to handle talks with kidnap gangs; and reducing the ransom from the initial asking price is an important part of ensuring the safe return of the victim.

Photography: iStock

Remote risks

Remote technology now allows surgeons to operate on patients who could be thousands of miles away. But how can such techniques be insured, asks **Marcus Alcock**

In 2010, British pensioner Kenneth Crocker, 70, had an irregular heartbeat corrected at the Glenfield Hospital in Leicestershire. But this was heart surgery with a difference. This was telesurgery, or remote surgery as it is otherwise known.

The procedure was conducted with a one-metre robotic arm that pushed a thin surgical tube into Kenneth's body while the surgeon, sitting in a separate room, used a remote control to steer it through a vein and into the heart to correct faulty tissue fibres. ▶

Illustration: Justin Metz

8,061
device malfunctions recorded in 1.7 million robotic operations

144
deaths were identified in the same sample of operations

Robotic surgery: Using robotics, surgeons can operate from remote locations and even from other countries

At the time, Kenneth's ground-breaking operation, completed in only one hour, was hailed an "enormous success" by doctors. The team claimed it was the first time the procedure had been carried out by a fully remote-controlled robot anywhere in the world.

Although that particular procedure was pioneering, the first use of a remote-controlled surgical device happened nine years earlier in France with the famous 'Operation Lindbergh' (see box on page 34). Although such procedures remain rare in the wider context of medical surgery, there can be little doubt that advancing technology will enable more and more operations to be carried out under the remote guidance of a surgeon.

Emerging technique

According to Matthew Clark, director of science and technology at insurance broker La Playa, this is still a science in its infancy. He explains: "I'd say telesurgery isn't that well established at the moment, but it is definitely an area that needs to be looked at. La Playa has a specialisation in life sciences and medical technologies. We don't have any robotic surgery clients at the moment but it's well within our gift and something we are interested in.

"It's a bit of a nascent market. Recent research shows the estimated value of robotic companies in this field in the US healthcare market will reach US$20 billion by 2021, but that's actually pretty small beer given the overall US healthcare spend. But as soon as it starts developing properly it could become significant."

Scott McFarlane, UK and Ireland life science manager at Chubb, agrees.

"There are existing specialist insurance programmes for life science companies that design and supply surgical medical products and robotics-based technology, and these are becoming more established," he explains. "So as of today surgeons are using robots to control surgery, but the idea of remote or telesurgery itself is new and upcoming, though it is increasingly being spoken about.

"Life science is merging with information technology and telecommunications, so more and more of that is combined with traditional life sciences risks, and that's an area we would expect to see continually develop."

Operational risk

Yet these operations carry a plethora of risks. Work carried out by researchers at the University of Illinois, the Massachusetts Institute of Technology and Chicago's Rush University Medical Center last year suggested that 144 deaths, 1,391 injuries and 8,061 device malfunctions were recorded out of a total of more than 1.7 million robotic procedures between January 2000 and December 2013.

> "These systems draw upon interconnected disciplines which carry an array of risks"

The paper was based on reports submitted by hospitals, patients, device manufacturers and others to the US Food and Drug Administration, with the study suggesting that the true number could be higher. Events detailed included broken instruments falling into patients' bodies, electrical sparks causing tissue burns and system errors making surgery take longer than planned.

Such reports are rare, especially for the European market. Matthew at La Playa says: "The difficulty from an insurance point of view is that there are low levels of data about the usage of robotic devices involved in telesurgery with regard to their efficacy and safety. There is a low level of statistical information for insurers to go on, so assessing the risks and pricing the insurance accordingly is the problem."

Matthew agrees that remote surgery has several potential problems for the insurance market. "I'd say there are a number of potential risks here," he says. "Things like including product liability or technical failure liability, if the system doesn't do what it is supposed to do. This will be critical.

"One also has to ask why hospitals would want to use remotely controlled robotic devices for surgery. One answer might be the savings involved, but if there is a financial loss, there could also be associated professional indemnity risks here," he notes, suggesting that clinical or product trials will be another area to look at.

Photography: Getty

"We need some information around the trial phase for these devices, so there will be associated clinical trials liability insurance," Matthew adds. "Also, these systems draw upon interconnected disciplines such as computer science, telemetry and virtual reality - all of which carry a complex array of risks. So there is a huge dependency on all of that working well."

The cyber threat

Other areas of concern that Matthew highlights include cyber threats - what happens if someone hacks into the system while a surgeon is using this technology? - and the risk around intellectual property. He says there is an increased amount of patient litigation around new systems and so the intellectual property area is likely to be a rich area for associated professionals.

> "There could be an added complication of the risks associated with the network"

According to Chubb's Scott, although remote surgery remains a relatively new field, insurers already have extensive experience with claims relating to medical and surgical devices. ►

> “There are low levels of data about the usage of robotic devices used in telesurgery”

device is the issues around the management of data or information held over a network, such as patient and medical records. This creates a potential cyber risk too.

Given the lack of data and the inherent risks involved, this might seem to be an area insurers will be uncomfortable with, but the reality is, as with any young market, it will take time for underwriters to adjust to the right level of cover for the risk and the appropriate terms and conditions.

Niche markets take time to bed down. Just think of directors’ and officers’ liability (D&O) insurance, which was once upon a time niche and is now a huge global market. Yet even the D&O market had some claims wobbles in the 1990s as it adjusted to the new risk landscape. Or think of wind turbines for renewable energy. It took underwriters some time to appreciate the level of operational risk associated with early turbine design.

Perhaps the telesurgery arena will be similar and brokers and underwriters need time to acclimatise. Even so, there is no doubt the appetite is there to take this new and exciting risk on board. As Scott says: “Across our life science and info tech segments, we write medical device, robotics and telecommunications risks, as well as patient record exposures, so it’s just a case of bringing all of these together.” ■

He says: “When we’re assessing any device used in surgery, we look at how it’s introduced to the patient, how established the technology is and its potential for injury. If injury to a patient occurs, the question of whether it’s as a result of the device or if it’s surgeon error arises.

“With telesurgery, there could be an added complication of the risks associated with the network being used, as well as the software and hardware involved in that connection. A downtime or delay in the network could have a significant impact. If an operation is being carried out and the network goes down, is there a surgeon on hand to take over?”

Scott points out that another risk with telesurgery and any networked medical

Telesurgery in brief

Surgical procedures carried out at a distance thanks to advances in robotic and computer technology and their applications to surgery are known as telesurgery, or remote surgery.

The first demonstration of transatlantic telesurgery was reported in 2001 when surgeons in New York operated on a 68-year-old woman in Strasbourg, France, and used remote-controlled robots to take out her gallbladder. It was named Operation Lindbergh after Charles Lindbergh’s pioneering transatlantic flight from New York to Paris.

France Telecom provided the fibreoptic lines, and Computer Motion provided a modified Zeus robotic system. After clinical evaluation of the complete solution, the human operation was successfully completed in September 2001. Surgical robot systems have since developed from the Zeus system and now include the da Vinci Surgical System.

Blast from the past

The explosion at Tianjin in China last year has some salutary lessons for risk managers, writes **Tony Dowding**

Every now and again a series of unfortunate coincidences takes place that results not only in a major disaster, but also in a real headache for those seeking to predict and manage risk.

Take the explosion at the port of Tianjin in China last year. The shocking accident not only resulted in more than 170 deaths, but insured losses that could end up pegged at between US$5 billion and US$6 billion.

The catastrophe happened when a fire broke out at a freight forwarder’s warehouse. The building was full of dangerous chemicals, far in excess of what was licensed. The fire brigade unknowingly put fresh water onto the chemical fire and two huge explosions followed. It then began to rain, causing the chemicals to react further and contaminate the entire area.

One of the biggest issues highlighted by the Tianjin disaster, which has affected both ▶

Photography: Getty

Photography: Getty

insureds and insurers, is accumulation risk.

Tianjin is a mega-port, handling mega-ships. As Phil Skelton, head of transportation risk management at Chubb explains, because these ships are so expensive to build and operate, they need to be filled. "There is a tendency to pack as much cargo as they can. So even if a shipper has booked his cargo in a number of containers over a number of days, the shipping line will try to get them on to one ship if they can. This means that while you are waiting for one of these mega-ships, you can get four or five days' worth of containers building up inside the port."

Building up a backlog

Phil says that if there is a slight delay with the ship, the containers may start to build up in the container yards outside of the main terminal. While the terminal is designed to handle containers coming in and out quickly, it is not designed for storage over a period of time. In Tianjin, the main container terminals were not affected – it was the container yards, where containers were either waiting to go into the port or had been unloaded and were waiting for distribution.

> "This will definitely have an impact on how people perceive accumulation"

The biggest loss at Tianjin involved over 10,000 cars, hit by both the explosion and the chemical contamination. One particular issue at Tianjin was that some of the car distributors didn't know how many cars were in the various stockyards around the port, making the claims process difficult for them. It was also difficult to assess the loss because the government put a blanket ban on access to the whole area, so nobody could get in to start assessing damage for four or five weeks.

Christian Stachel, Chubb's marine claims manager for continental Europe and Eurasia, says: "An added complexity was that, in some cases, it was not entirely clear to whom the cars belonged. Were they already sold? Did they still belong to the insured? If a car was damaged by fire, it is a total loss. But if it is minor damage, will the insured take the risk of selling potentially contaminated cars into the market or not?"

The size of Tianjin port and the extent of the disaster means the issue of location has become a focus of debate. Christian explains that in the contracts he is dealing with in relation to Tianjin, the definition of location is not clear. "There were several addresses in Tianjin that were affected, and it could be argued that Tianjin port is the location – the whole area – or it could be argued that each single address is one location. Is the location the whole area of Tianjin port? Or is it each single address?"

Scale of the problem

Trevor McGarry, executive director of marine insurance at Willis, says: "Nobody in the market realised that Tianjin was so huge. Some people had cars in seven or eight different locations in Tianjin. Typically, something like a hailstorm or windstorm would be highly unlikely to affect all of those locations, as they are quite localised. But with this explosion, all the locations were affected. Nobody had envisaged this. It will definitely have a lasting impact on how people perceive accumulation.

"I am aware of several accounts where underwriters thought they were writing a US$30–US$40 million limit, but it turns out they have seven or eight locations at Tianjin. As a result, I think we will see, perhaps on the marine side, a move to a per occurrence basis rather than per location."

Trevor adds that most of Willis' clients he has spoken to had more cars in Tianjin than they had anticipated. The Chinese economy had slowed down and there were more cars stored in the port than people expected. To make things worse, the explosion was close to the main vehicle storage area.

"Vehicles are much more exposed and vulnerable than something that is in a container," Trevor adds. "Having said that, Willis has a client that had foodstuffs in a container several kilometres away, which suffered contamination. There were cars stored ten kilometres away that ended up with contamination."

> "It is important to have clarity over what is insured and what is not"

Photography: Getty

So what are the lessons from Tianjin? Phil says the issue with accumulation is to not have too many eggs in one basket in a single location. He says it is about managing the supply chain so that goods are filtered into the port or onto the ship at the last possible moment.

Out of control

The difficulty is that the risk manager has little control or influence over this. It is organised by logistics departments and logistics service providers. Phil continues: "Talking to the risk managers of some of the big companies, even they – or their organisations – don't know what is moving at times because they have so many subsidiaries and purchasing arms.

"You can start to build up an accumulation unknowingly. Being aware of the accumulation risk is something we have been pushing with insureds for a number of years. Some of the logistics providers have got the software to monitor what is in transit but some haven't. That is the problem."

It is also important to have clarity over what is insured and what is not. Christian at Chubb says: "The most important lesson from Tianjin is to have a really clear picture as to when the risk transfers from one business to another. If you have a car shipped to China, for example, the ownership is transferred to the buyer. It is important to be precise at what point the transfer happens. It is not just a clear insurance contract but also a sales contract without ambiguity. Businesses will never know what their exposure is if they are not clear when ownership transferred to the buyer."

Tianjin, an unprecedented chain of unexpected events and consequences resulting in accumulation risk, provides an important lesson for risk managers about the value of contingency planning and, of course, insurance. The unexpected can go wrong and the consequences can be severe. And that is exactly what insurance is designed for. ■

Tianjin's lessons for risk managers

Be aware of accumulation risk
Know where your goods are or get your logistics provider to track them – though, of course, this is easier said than done. To help with the issue of accumulation, it can be important to know which ports are being used for your goods.

Reduce storage time
Reduce the amount of time that your goods are stored at ports if possible. This might mean ensuring that goods are delivered into the port at the last moment so they are taken to distribution centres away from the port as soon as possible.

Value of contingency planning and insurance
Tianjin emphasises the value of contingency planning. Where would you deliver your containers as an alternative? What is the next available port? Are some products so sensitive that air freight may be required to maintain orders or a factory's production? Insurance has a major role to play but it is vital to define the maximum exposure and ensure the limit and wording are clear in any circumstance.

Get in touch

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

Protected from grape to glass

Making fine wine is a delicate business with a surprising number of pitfalls

20,000
the number of bottles a single vat can hold

16–17°C
the temperature at which wine should be stored – variations can damage it

Think of fine wine, and the greatest hazard some might expect is a woozy head the morning after a particularly thorough tasting. And yet, for cellarmasters in regions such as Bordeaux, the journey from grape to glass is beset by a host of risks. Understanding these helps Chubb support vintners all over France.

If someone deals with wine day in, day out, you might think that putting a cork in it comes naturally. But speaking to Bruno Jacquet, senior property underwriter for France at Chubb, it is not so.

"In our experience, the biggest risk that wine producers in the Bordeaux region – and, indeed, the world – face is the loss of wine from the vats in which it's vinified and stored," he explains.

"This happens when containers or valves haven't been closed and locked properly, or from leakage on flexible pipes and taps used during pumping operations. We come across this kind of disaster quite often. Nowadays, the loss of stock through spillage is much greater, due to the steep increase in the market price of Bordeaux wine in the last decade. A single vat can hold, on average, the equivalent of 15,000 to 20,000 bottles, worth several hundreds of thousands of euros."

Bruno explains: "What causes these accidents is usually human error. We had a case once where someone accidentally crashed a forklift into a vat – this kind of risk could have been avoided by installing barriers."

Small mistake, enormous damage

Sébastien Bardinet, managing director of insurance brokers Duchesne, agrees: "Wine producers dread this kind of disaster the most, because, psychologically, it's like watching the fruits of a year's labour going down the drain. Most growers now try to be very vigilant. We recommend for instance that, at the end of a day's work, they check over all of the tanks to ensure that they're fully closed, and that there isn't a leak in any of the taps. Additionally, some wine producers are beginning to replace their old vats with more modern, smaller ones that hold lower volumes of wine, which reduces the amount lost through spillage."

> "The biggest risk that wine producers face is loss from the vats in which it's stored"

A pioneering policy

"Historically," explains Sébastien, "traditional insurers were prepared to cover damage to buildings and materials, but they didn't like covering the wine itself. Chubb came up with the idea of a package that centred around insuring the wine. So now we have an excellent track record in the field."

These days, some insurance companies will not only cover businesses for mopping up after an event, but also work with them to prevent any oenological calamities from happening in the first place. They have engineers who can visit companies at a very early stage in construction projects. They advise on specific risks and intervene to ensure that the right conditions are put in place.

Policies often now protect against flooded cellars. And while there are generally more floods, the châteaux of Bordeaux – perching majestically on hills – remain mercifully high and dry.

"Flooding can be more of a problem for wine merchants because they historically have stores and warehouses on embankments, and so are exposed to the risk of rivers – in this case, the Garonne – overflowing," explains Sébastien.

When the floods wash away the labels of expensive bottles, that's a real problem for merchants, he adds.

"If you lose the label off bottles of Château Lafite, you can't simply order another batch: only the vintner is authorised to do that. However, producers are extremely reluctant to release more labels, because they worry about counterfeit bottles being produced. Plus, even if the labels were released, merchants would have to cover the costs of reprinting the labels and repackaging the bottles."

Fine wine has always been a target for thieves. To deter them, vineyards have started storing bottles without their labels on: this dramatically reduces their value.

"Security against theft has improved greatly over the past decade thanks to the wider availability of increasingly effective mid-range electronic security systems," says Bruno. "The combination of alarms with video surveillance has reduced the likelihood of robberies; and most of those that take place don't result in such significant sums of money being lost, partly because it's time-consuming to transport that number of stolen bottles. It also helps that, nowadays, people outside the business, such as delivery people and lorry drivers, aren't allowed access to the wine stores."

Designing out risk

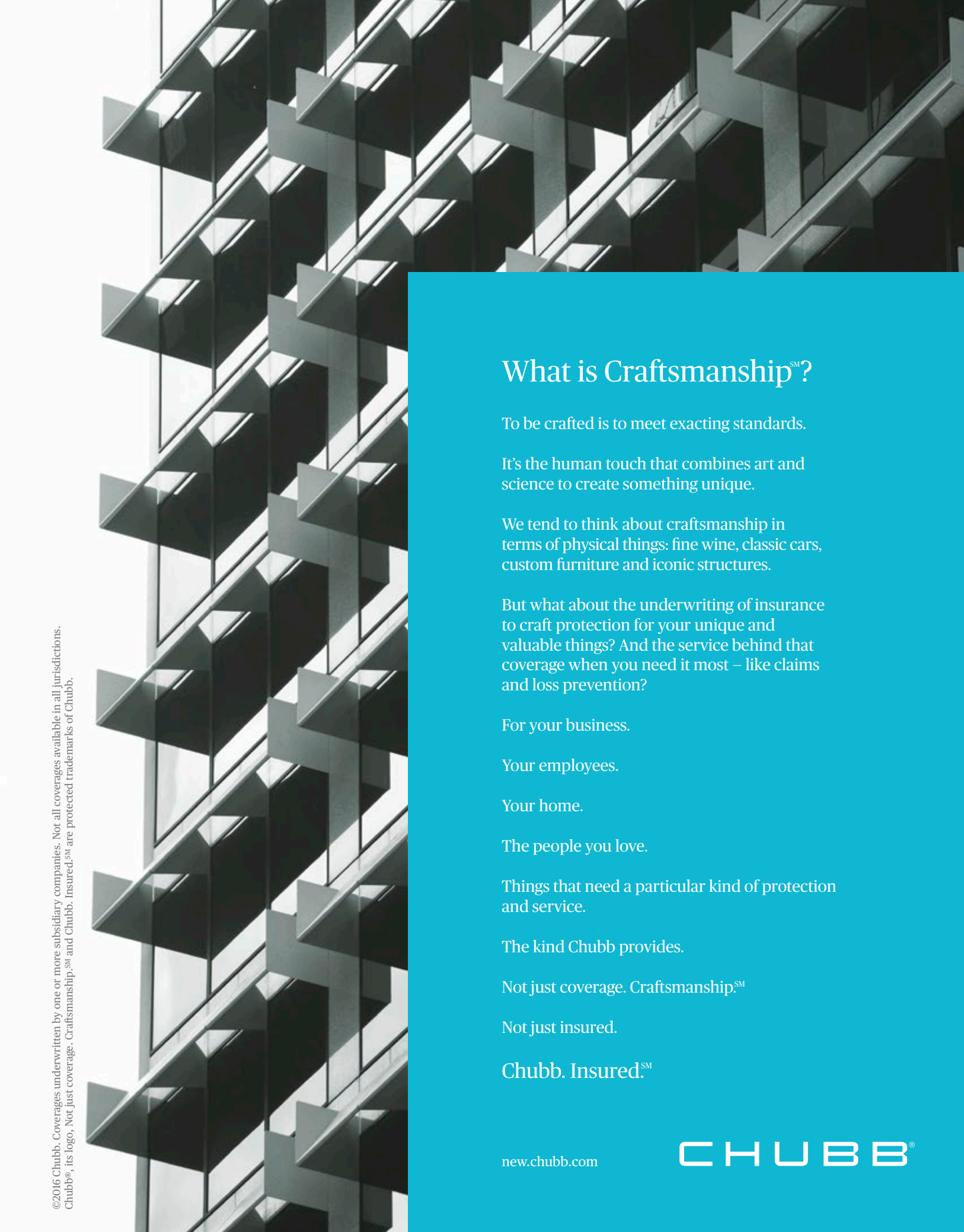
It's the design of these stores themselves that is crucial when it comes to keeping wine safe. "Variations in temperature can damage wine; it should be stored at between 16 and 17°C," explains Bruno.

In the past, says Sébastien, the use of polyurethane or polystyrene as insulation material was not uncommon. The problem is that the material is flammable and releases toxic fumes, which are then absorbed by the wine.

Modern warehouses are not only built using non-combustible insulation material, they also control temperature and humidity. This is a great help in modern buildings, where the environment is less stable than in the cavernous cellars of historic castles.

Modern vats also control temperature. But this technology has its dangers. The coolant, glycol, can accidentally contaminate the wine and make it undrinkable. Contamination can also occur due to faulty equipment: in one case, a malfunctioning bottling machine caused tiny shards of glass to pollute the wine. The vineyard's laboratory spotted the contamination early on: nevertheless, bottling had to be stopped, the affected lots recalled and the machine repaired. The affected vintner's insurance covered all these costs, as well as the replacement cost of the spoilt wine at market prices.

Teetotallers may sneer that it's all rather a lot of fuss over a bit of fermented grape juice. But if you're one of the many connoisseurs who enjoy a bottle of Château d'Yquem in good company, perhaps you'll raise a glass to the people who watched over its production. ■



What is Craftsmanship℠?

To be crafted is to meet exacting standards.

It's the human touch that combines art and science to create something unique.

We tend to think about craftsmanship in terms of physical things: fine wine, classic cars, custom furniture and iconic structures.

But what about the underwriting of insurance to craft protection for your unique and valuable things? And the service behind that coverage when you need it most – like claims and loss prevention?

For your business.

Your employees.

Your home.

The people you love.

Things that need a particular kind of protection and service.

The kind Chubb provides.

Not just coverage. Craftsmanship.℠

Not just insured.

Chubb. Insured.℠

new.chubb.com

CHUBB®