Risk Management Technology

Monday October 3 2016

www.ft.com/reports | @ftreports

Insurers rush to grab hold of start-ups with potential

Traditional players hope to take advantage of innovators' tech know-how, writes *Oliver Ralph*

Making strides: outside the head office of Munich Re, which has partnered with Trov — Ulrich Baumgarten/Getty Images

Autumn started with a rush of deals. As August turned to September, a clutch of big insurers announced investments in start-ups. Allianz put funds into MoneyFarm, a digital wealth manager. Munich Re partnered with Trov, which is developing a range of on-demand insurance products. Axa backed Gasolead, which is creating a virtual assistant to help insurance agents generate more digital leads.

If this is an industry playing catch-up on tech, it is playing hard. "[Insurers] are working closely with start-ups rather than seeing them as a threat," says Nigel Walsh, a partner at Deloitte.

For others, however, there is a long way to go. Tom Butterworth of Silicon Valley Bank, which finances early-stage companies, describes the sector as archaic. "It's seen as the laggard in adopting new technology," he says.

The September deals showed the breadth of technologies in which insurers are dabbling as they look for new ways to help customers — both retail and corporate — manage risk.

Telematics is particularly popular. What started as the ability to assess how well young people drive via a black box in the car is quickly expanding into a range of similar ideas. Health insurance linked to fitness devices is one. Home or factory insurance policies linked to various types of sensor are another.

Data analysis is a hot topic. "The insurers are probably a bit more mature than the banks in using big data to drive value," says Roy Jubraj, managing director at Accenture. The idea is that, by analysing data, insurers can assess risk more accurately. This is not always straightforward. UK regulators recently looked at whether insurers' use of data could harm consumers, although it eventually decided that the issue did not merit a full investigation.

Meanwhile, blockchain, the technology behind bitcoin, is never far from the discussion. Insurers are investigating how it could make insurance contracts cheaper and more secure. "Blockchain has the opportunity to fundamentally change the way we interact with insurers," says Mr Walsh. He adds that smart contracts — which pay out automatically if something happens, without the policyholder needing to make a claim — are one way in which the technology could change the industry.

Yet there are limits to how far big, traditional insurers can go when it comes to making the most of new developments. "Legacy systems are holding them back quite a bit," says Mr Jubraj. "That's why major players are embarking on new platforms, modernising what they have."

Old technology, says Mr Jubraj, hinders insurers' ability to create new products quickly. "Today most insurers push digital services based on the products they are [already] selling. Not many are looking at you as a customer and driving a proposition around that, as Amazon has in retail," he adds.

That is where a lot of the start-ups come in. New entrants are selling variations on traditional policies — car insurance by the mile, for example, or cover for specific possessions. By combining with these start-ups, insurers win some underwriting business (very few start-ups are fully licensed insurers) and get an early peek at which sorts of products might work well.

"For the foreseeable future, barriers to entry are so huge that you'll see this layer added to the top of the industry," says Mr Butterworth. "It is the [insurers] most willing to integrate with the early-stage companies that will come out on top."

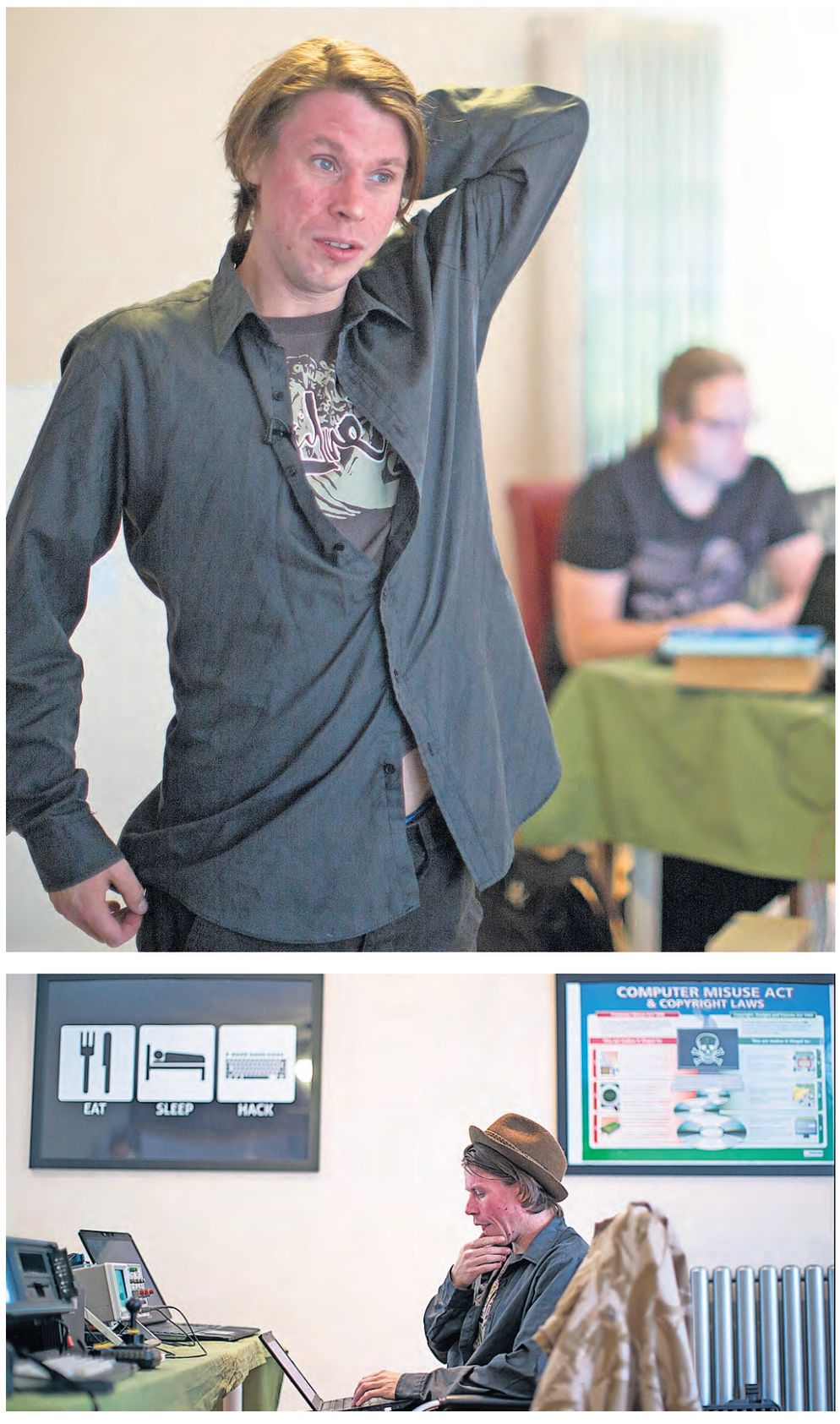
Cyber insurance is one exception. Multinationals including AIG, Munich Re, Allianz and Beazley have pushed into cyber. Analysts say it is one of the few areas of commercial and wholesale insurance that offers much growth. Adoption is much higher in the US than Europe, but EU rules coming in 2018 are expected to boost take-up.

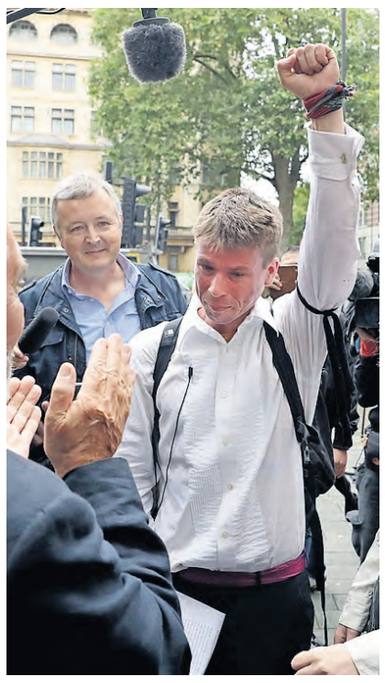
However, customer demands are changing in cyber. While cyber policies traditionally cover companies for financial and operational problems caused by data loss, industry surveys suggest that policyholders have a wider range of worries, such as what happens if a cyber attack causes physical damage, or the consequences of a hack that affects products. The question for insurers is how quickly they can model and price those risks.

Inside

Cyber poacher turns gamekeeper

Interview
Lauri Love
The British hacker facing extradition to the US talks to *Maija Palmer*





If businesses are serious about reducing the risk of cyber attacks, they must work closely with hackers, says Lauri Love, the UK computer security expert who is facing extradition to the US, accused of computer crimes.

Mr Love, who lost his appeal against extradition in September, says more should be done to ensure young people with computer skills learn to use their talents in a positive way working for companies, rather than engaging in crime. The transition to cyber vandalism and worse often starts when a bright but socially awkward teenager is drawn into the wrong circles, he says.

"A lot of the mental make-up that can make you quite good at analysing computers and information systems tends to manifest with problems of social adaptiveness. People can find that they have trouble concentrating at school or problems with behaviour and authority," Mr Love adds. "They don't have the availability and means of getting into doing cyber security and developing their skills in the appropriate safe environment in a constructive way.

"The underworld doesn't care how well-dressed you are or whether you can maintain eye contact. They just care if you have the skills. There is a perverse sense in which the criminal underworld is more meritocratic than society. Sadly, their agenda is different."

Until last month, Mr Love was part of a social enterprise, Hacker House, which aims to give young computer enthusiasts a place to practise their hacking skills without causing damage — and to put them to use helping, rather than harming, businesses.

"We want to provide a place where people who have started down the path to being a little bit naughty can come. We can say, 'OK, we will teach you how to hack, you can have all the fun, but you won't be interfering with someone's business and you won't find yourself on the end of a difficult conversation with people with badges,'" he adds.

Companies could learn a lot from hackers, Mr Love says. Most businesses severely underestimate their risk from cyber crime. Hackers often penetrate their defences in very basic ways.

"There is a lot of code running on computers — some of it is kept up to date and patched against security vulnerabilities, some of it is not," Mr Love says. "Hacking is mostly a case of persistence; it is not always a case of spectacular ability — just determination to keep looking until you find the one thing that wasn't up to scratch."

He compares looking at the back end of corporate systems to looking back in time. "Sometimes you end up going back to the 1990s and finding levels of security that we ought to have moved past," he says. "You see the same mistakes over and over again."

There is a tradition of ex-hackers going to work in corporate security. Kevin Mitnick, who was imprisoned in the US in the 1990s for hacking, runs his own corporate security consultancy. George Hotz, a hacker who faced litigation by Sony in 2011 for hacking the PlayStation 3 games console, has since worked for Facebook and Google.

Companies can also tap into the hacker community more broadly by setting up so-called "bug bounty" programmes, where hackers are rewarded if they discover and report serious security flaws.

"We can shape the rules of the game so people who find these things out have a way to come to the [company] and say, 'I have found out this is insecure,' without being afraid of being prosecuted or sued," Mr Love says. "We can create an incentive structure to bring people onside. These are bug bounty programmes and people are just learning to do them."

With a mischievous smile, Mr Love, who is accused of breaking into US military computers, adds: "In fact the Pentagon just ran its first bug bounty system. And so whereas some people in the world are in trouble for allegedly hacking the Pentagon, now the Pentagon is asking sometimes the same people to come and hack it."

Penetration: Lauri Love at Hacker House — where he used to work — and, top right, outside court after losing his appeal against extradition
Charlie Bibby/AP Photo/ Matt Dunham

The FBI and US Department of Justice allege Mr Love stole thousands of files from the Pentagon and Nasa, as well as from other bodies, including the Federal Reserve and Environmental Protection Agency.

Mr Love's lawyers have argued that he should face legal proceedings in the UK rather than the US, where they say his health could be affected by a lengthy jail term. Mr Love has Asperger syndrome, which his lawyers say could deteriorate and lead to a mental breakdown or even suicide.

In any case, Mr Love feels the current approach by the police and criminal justice system is not deterring hackers.

> 'Hacking is mostly a case of persistence; it is not always spectacular ability'

"The issue is that there are 7bn people connected to the internet and not all of them are in legal jurisdictions where computer crimes will be prosecuted. Even if you can scare all the people in the UK into not testing your security, that doesn't affect the people that live somewhere where you don't have extradition arrangements," he says.

He is not arguing that computer breaches should be decriminalised, but he says there should be more differentiation between cases where hackers are going in to steal money or information, and cases where people are merely testing the system's defences.

"When you damage a system, when you trespass, when you interfere with business operations — that is a crime and should remain defined as a crime. But the priority of the state shouldn't be to try to frighten people into not testing security, we need security to be tested," he says.

"I don't think we should be heavy-handed with people, not when they haven't adopted a criminal mindset. I'm hoping law enforcement can start taking more of a harm-reduction approach rather than this kind of traditional drugs-war approach of being very hard on it and trying to scare the kids straight — because the kids aren't being scared straight."

Mr Love's case is due to considered by Amber Rudd, the UK's home secretary, in mid-November. If she decides to authorise the US's extradition request, Mr Love will have 14 days to appeal against the ruling.

How I protect my online identity

COMMENT
Violet Blue

Every time I sign up to a website or app I know I'm gambling with my personal security. Being spammed by a company's mailing list has gone from my biggest sign-up stress to the least of my worries. Questions hammer my nerves with every piece of information I hand over. Are the company's databases secure or are intruders lurking in the wires? Will it tell me who it is selling my information to? Will its product infect my computer or phone with malware? I can Google the company's security record, but do I really want to? Would it be truthful anyway, or just PR?

I try to interpret signals in the sign-up process. The fractured negotiation begins with my email address and ends with the background information I know the company is recording from my phone or computer. I try to suss out which parts of the form I'm filling out I can fib about, and which could mess up my use of the product.

I'm not alone. Digital security is out of hand — just ask the holders of the 500m hacked Yahoo accounts. Nearly 5bn records have been lost or stolen in all known breaches since 2013, according to digital security specialist Gemalto.

Depending on how much I trust any given website or app (which is about how much I trust any total stranger — not at all, no matter how well-designed they seem), there are several things I do to shore up my shaky digital security. I never use my most personal email address for sign-ups — that's what my three "dummy" accounts are for. The same goes for my phone number. I have a business mailing address, which ensures my home hasn't been in anyone's databases for several years.

> 'Digital security is out of hand – just ask the holders of the 500m hacked Yahoo accounts'

I take things further if a situation looks especially shady. I use something called a VPN, or virtual private network, which is easy to buy and install. It essentially lets me flip a switch and send location information — my IP or internet protocol address — via another computer somewhere else in the world. I do this when I don't want a site to know even generally where I live.

I encrypt my laptop's hard drive, I use two-step verifications for logins whenever the feature is available, I make all my devices password-protected and I never sign in to any account on someone else's device.

Since hacking groups such as OurMine started combing through billions of breached records and stealing users' passwords to see what works in other services, I have used a password manager called 1Password to find any duplicate passwords across my accounts and change them. I also keep a little sticker over the cameras on all my devices to prevent unauthorised spying. Programs that spy through webcams are cheap and fairly simple to use.

Other people's bad security isn't the only thing we need to look out for. Malvertising, where online ads spread viruses and worse, have been found on the biggest websites, including the New York Times and the BBC's US site, which hosts ads. Tainted ads have been known to pass on malware, spyware and dreaded ransomware — where files are encrypted and held for ransom. The best defence against malvertising is always using an ad-blocker in your browser.

Ransomware also spreads through infected email attachments and links. For this reason, I tune my email settings so that they never do anything automatically, such as show images or download attachments. I also keep a back-up of my important files on a hard drive that is not connected to any network.

So far, so good on this side of the screen. But I might occasionally throw a little salt over my shoulder. Just in case.

Violet Blue is a personal online security expert and author of The Smart Girl's Guide to Privacy.

Small companies are not immune to costly attacks

Security

Just under half of such businesses have adequate cyber insurance coverage, reports *Bradley Gerrard*

Managers of small and medium businesses who assume that only the biggest companies are targeted by cyber attacks have already made their first mistake.

A third of small British businesses suffered a cyber breach in the past year, according to a UK government study, while just under half of such companies had any form of cyber insurance cover.

Yet the government study showed 60 per cent of small businesses had cyber incident response plans in place, compared with 52 per cent of all companies.

Dave Palmer, director of technology at cyber security consultancy Darktrace, says many attacks are indiscriminate, so it is essential that executives of companies of all sizes "think about the risks of what would kill the business and stop it operating" if a hack or data theft occurs.

Mark Hawksworth, head of the technology practice at Cunningham Lindsey, a loss adjuster, says hackers are increasingly targeting smaller businesses because larger employers have more resources to protect themselves, making smaller companies more vulnerable.

One form of cyber attack that is becoming more common, and to which smaller companies are particularly exposed, is the use of ransomware. This is where the attacker gains entry to a company's network, encrypts the data and makes them unusable, then demands a ransom from the company in return for an encryption key.

Insurer Beazley predicts a 400 per cent increase in ransomware breaches globally this year. Businesses cannot be entirely immune from such attacks, security experts say, but there are several simple and practical steps to help reduce the risk.

These include ensuring employee passwords are long and difficult to guess, training staff to recognise unsolicited emails and — most importantly — keeping technology up to date. "There can be a desire to sweat assets, but it is important to keep computers and software updated," says Mr Palmer.


Ransom beware: Dave Palmer

Another measure cyber security specialists advise smaller companies put in place is software that spots unusual network activity, such as bulk copying to an external hard drive. Mr Palmer says he has seen a spate of incidents recently where the culprits were disgruntled employees stealing data.

Sandra Cole, UK and international breach response manager at Beazley, says regardless whether a company has cyber insurance, it should have an incident response plan in place. This means that in the event of a breach staff are given roles such as contacting clients and authorities, "rather than running around like headless chicken," Ms Cole says. The plan needs to be tested and updated rather than just drawn up and forgotten about, she adds.

Mr Hawksworth says small businesses often use external IT consultants to keep down costs, but suggests they appoint someone internally to make sure IT policies are adhered to and put them in charge of the response plan in the event of an attack.

Old tech opens door to hackers

Legacy systems

Security focus is shifting to make it harder for intruders to leave with anything of value, writes *Angus Batey*

Outdated technology often acts as a company's soft underbelly, leaving them open to cyber breaches. But the cost and inconvenience of moving from so-called legacy systems means such vulnerabilities are hard to address.

Companies and security providers are gradually realising that it is impossible to build impenetrable defences and keep out every attacker. Instead, the focus has shifted to ensuring that once a system has been compromised it is difficult for an intruder to leave with anything useful.

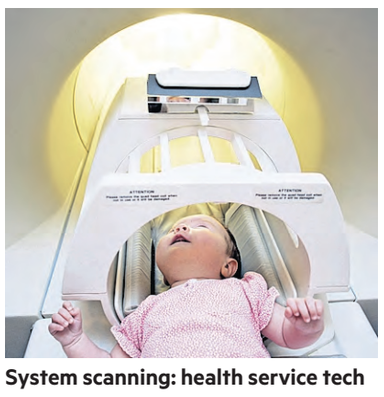
According to Net Applications, a web analytics company based in California, the third most widely used desktop computer operating system in the world is Windows XP. It is run on nearly one in 10 desktop computers even though Microsoft stopped writing and distributing security updates for it in 2014.

For many companies, the cost of replacing software for their entire stock of computers is prohibitive, even without factoring in the disruption it would cause. There are other issues to consider, too. Sometimes the legacy system may be running on computers housed inside expensive specialist tools. This is particularly true in industries with budget pressures such as healthcare.

Dan Taylor, head of cyber security at NHS Digital, the body that advises the UK's National Health Service on cyber security, says the use of Windows XP persists in some unexpected parts of the NHS because of this problem. "You wouldn't throw out your MRI scanner because it's got XP," he says.

> 'Businesses are realising it's about how you respond to the security breach'

Businesses — both those running legacy systems and the security consultants helping them with their data security — are learning that the most practical solution often involves accepting some level of security risk.


System scanning: health service tech

"In the past, the approach was to do nothing: the security challenge didn't outweigh the risk of bringing the enterprise to a halt," says Salvatore Sinno, chief security architect for Europe at IT company Unisys. "Now the approach is around three fundamental strategies: hardening the legacy systems; doing a formal risk assessment of a particular system to identify what elements are most at risk, and replacing that part of the system; and, in some industries, replacing the legacy system completely."

Mr Sinno says there are several options open to organisations unable or unwilling to replace legacy systems.

"Businesses are putting more effort into having a better understanding of what damage security incidents can do," he says. "At the same time they are starting to realise that it's [about] how you respond to the security breach."

An anonymous reporting culture can help organisations learn from cyber security mistakes, but just as vital is an awareness of the extent to which legacy systems are still in use. "If you count pharmacists, there are 40,000 NHS organisations," says Mr Taylor, who is trying to find out how many of them still use Windows XP. "What we don't know is the scale of the problem. Once we know . . . we can work out the different strategies to move them off [legacy systems] as soon as possible."

‘Insurtech’ start-ups that are causing a stir

Innovation
Links between traditional insurers and new players are critical for both. By *Oliver Ralph*

For a long time, the fintech start-up scene took little interest in the seemingly sleepy world of insurance. Payments, foreign exchange and peer-to-peer lending grabbed the headlines, plus the funding.

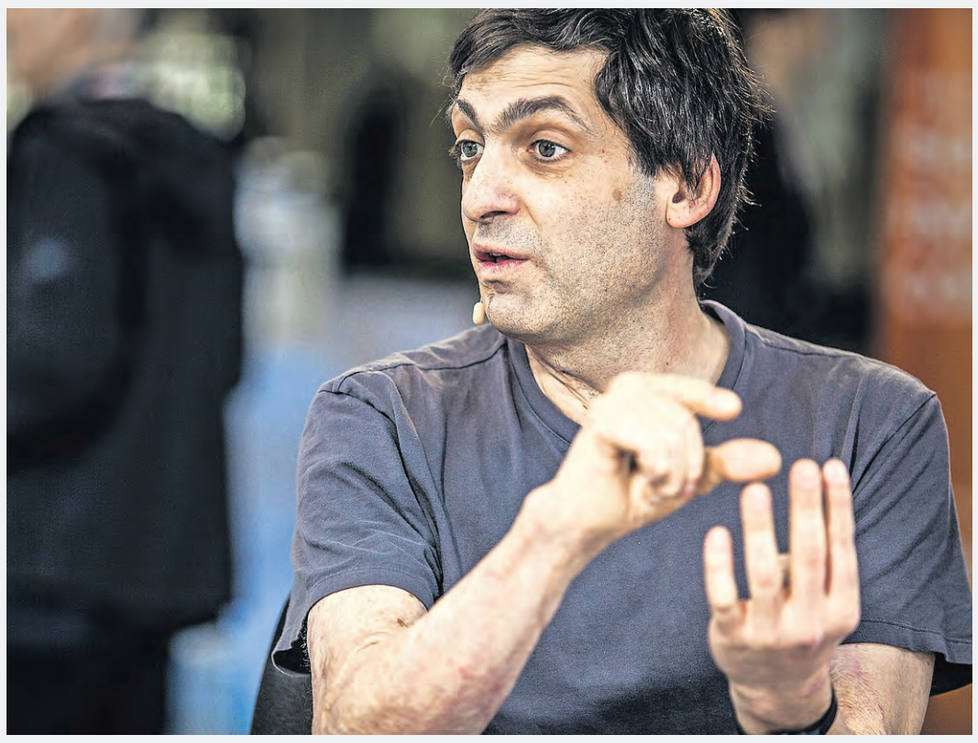
But over the past couple of years, all that has changed. Insurtech — or instech — is now attracting entrepreneurs and the investors that back them. “Quite a few entrepreneurs who have been in other areas of fintech have moved over to insurance,” says Matthew Wong of research company CB Insights.

Funding for insurance technology companies rose from $740m in 2014 to $2.7bn a year later, according to CB Insights. This year has also been busy. “Deal pace is higher than it was last year,” says Mr Wong. “There’s a lot more enthusiasm, especially at the early stage.”

The start-ups are targeting all parts of insurance. Many are focusing on distribution, using new technology to reach consumers that traditional insurers miss. Others are looking at analytics, helping insurers to use data to make better underwriting decisions. Blockchain — the technology that underpins bitcoin — is increasingly popular, while health insurance has been a big area of start-up activity in the US. Nor have start-ups ignored the potential of the “internet of things” — the growing use of data-collecting devices in everyday items, from cars using telematics systems to connected homes.

Few start-ups have become full, risk-bearing insurers. Analysts say that the capital requirements, regulatory burden and complexity required, combined with the desire of investors for short-term returns, means that very few of them underwrite their own policies. The result is that for most start-ups, partnerships with existing insurers are critical. Without them, many would struggle to make the business model work.

Insurers tend to be willing partners, seeing start-ups as a way to win business in normally out-of-reach markets. But Nigel Walsh, partner at Deloitte, warns of drawbacks. “The risk is that the insurers will have no interaction with their clients,” he says. “They’ll just be product manufacturing.”



◀ **Pictures (clockwise from top left): Cuvva for rarely used cars; Dan Ariely; US health workers; Robin von Hein**
Richard Baker/Getty Images/Chris Goodney Bloomberg/ Andreas Lukoschek/Brendan Smialowski/AFP

Cuvva

Founded: 2014
Founders: Freddy Macnamara and James Billingham
Shareholders: Angel syndicate
Funding: £500,000
Based: UK
Activity: Cuvva takes a fresh approach to car insurance. While most insurers cover customers’ vehicles for a full year, Cuvva breaks it down into smaller chunks. Its first product allows policyholders to insure themselves on a friend’s vehicle for as short a period as an hour via an app. Its second, to be launched this autumn, will allow drivers to buy an hour of coverage for their own vehicles, which is designed to suit people who do not drive frequently. While Cuvva is still at an early stage of development, some analysts say that insurers will increasingly have to follow its model of offering more flexible products than their current range of fixed, year-long contracts. Cuvva uses data provided by the UK’s Driver and Vehicle Licensing Authority to help verify policy requests, a process that takes about 10 minutes.

Cyence

Founded: 2014
Founders: Arvind Parthasarathi and George Ng
Shareholders: New Enterprise Associates, IVP and Dowling Capital Partners
Funding: $40m
Based: US
Activity: Demand for cyber insurance has been growing rapidly over the past few years, with high-profile attacks on companies such as Target in the US and TalkTalk in the UK persuading companies that they need cover. For insurers, cyber offers plenty of potential growth but also lots of uncertainty. How likely is it that any given client will be hacked — and, if they are, how much damage could there be? San Francisco-based Cyence is developing a system that can model these risks in financial and economic terms. It has already won its first customers, including Brit Insurance, AM Best and Marsh. In September it raised $40m from investors in one of the largest insurtech fundraisings of the year.

Lemonade

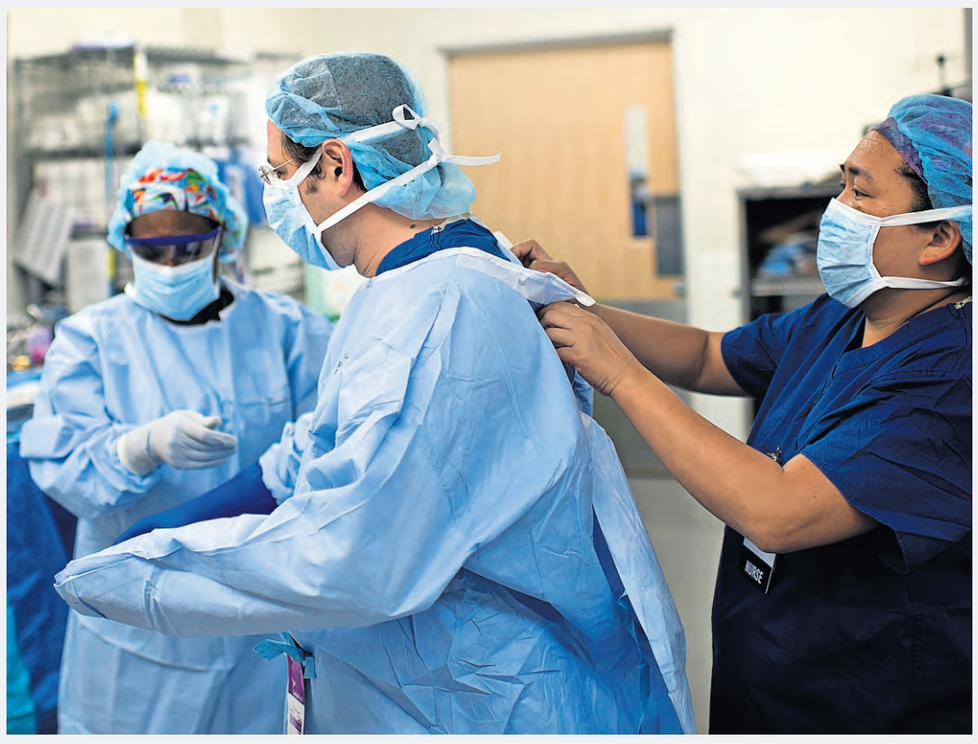
Founded: 2014
Founders: Daniel Schreiber and Shai Wininger
Shareholders: Sequoia, Aleph and XL Innovate
Funding: $13m
Based: US
Activity: Lemonade has been the subject of speculation. It first billed itself as a peer-to-peer insurer, but was coy about exactly what that meant or its business model. It has since raised money, signed partnerships with the likes of Berkshire Hathaway, Lloyd’s and XL Catlin, and recruited high-profile executives. It even hired behavioural economist Dan Ariely, author of bestseller *Predictably Irrational*, as chief behavioural officer. In September the company, which unlike many other insurtech start-ups is licensed as an insurer, revealed it will sell home insurance in New York. It will group its customers together and, at the end of each year, any premiums that have not been paid as claims will be given to a charity of the group’s choosing.

Oscar

Founded: 2012
Founders: Mario Schlosser and Josh Kushner
Shareholders: Fidelity Investments, Google Capital, General Catalyst, Founders Fund, Lakestar, Khosla Ventures and Thrive Capital
Funding: $750m
Based: US
Activity: Oscar is one of the older and more developed insurtech start-ups. Focused on health insurance, Oscar uses technology and data to improve the care it offers to its customers. It was created after the introduction of the US Affordable Care Act, known as Obamacare, and its services are available in New York and New Jersey. Among the benefits it offers are phone lines to its doctors and systems that help healthcare professionals manage members’ care. It has some big-name backers, including Fidelity and Google, and a fundraising earlier this year valued the company at almost $3bn. According to Deloitte it has annual revenue of $200m.

Policygenius

Founded: 2014
Founders: Jennifer Fitzgerald and Francois de Lame
Shareholders: Revolution Ventures, Karlin Ventures, Susa Ventures, Transamerica Ventures, Axa Strategic Ventures and MassMutual Ventures
Funding: $21m
Based: US
Activity: Price comparison sites have been in the UK for many years, regularly assaulting potential customers with TV ads featuring meerkats, opera singers and other outlandish characters. But the US market has been slower to take off. Analysts blame a reliance on brokers for distribution, state-by-state regulation and wariness from customers and insurers. Policygenius is hoping to help change that, arguing that more and more Americans would rather organise their insurance online than via an agent. It offers a range of products including life, health and pet policies. With backers such as big insurers Axa, Transamerica and MassMutual, it could make a dent in the market.



Safeshare

Founded: 2015
Founders: Alexander Steinart
Shareholders: Founder and Z/Yen
Funding: £200,000
Based: UK
Activity: Blockchain is one of the buzzwords of the fintech world, and this is no different among insurers. The technology allows transactions to be recorded securely in multiple locations. How exactly it can be used in insurance is the subject of much discussion within the industry. Safeshare is one of the few companies to have launched a blockchain-based product. It describes its market as “insurance for the sharing economy”, and its first product illustrates what it is trying to do. In March it announced it had teamed up with Vrumi — a website that allows people to rent out their spare rooms for use as offices — to launch property insurance. The policies are underwritten at Lloyd’s and the use of blockchain should, in theory, allow the parties involved in the policy to be linked securely and cheaply.

Simplesurance

Founded: 2012
Founders: Robin von Hein, Joachim von Bonin and Ismail Asci
Shareholders: Rheingau Founders, Assurant, Route 66 and Allianz SE
Funding: €20m
Based: Germany
Activity: One of the big hopes for insurtech is that it will break insurance down from the catch-all policies insurers have traditionally offered into more specific coverage for individual needs. Simplesurance is one of the companies aiming to do that by allowing people to buy insurance for products at the point of sale. Although smartphones, laptops and tablets dominate, it can be used for a much wider range of items. Founder Robin von Hein says the company has almost 2,000 ecommerce providers using its system, and that it launches in a new country every four weeks. Like other start-ups, Simplesurance is not a risk-bearing insurer itself. Instead it acts as a broker, passing on the risk to traditional players such as Allianz and Assurant.

SPIXII

Founded: 2016
Founders: Alberto Chierici, Renaud Million and Alberto Pasqualotto
Shareholders: Founders
Funding: Under £50,000
Based: UK
Activity: A relatively new start-up, SPIXII was founded by a group of former actuaries and computer scientists, one of whom used to be a consultant for high-frequency trading firms. Like many insurtech start-ups, its target is the way insurers interact with their customers. SPIXII is developing a chatbot — software that allows insurers, brokers and price comparison sites to talk to customers via programs such as Facebook Messenger and Skype. It is still early days, but SPIXII’s founders say that within four months of launching it had a pipeline of more than 60 companies that were interested in its technology. It has also caught the attention of Germany’s Allianz, which has put SPIXII into a five-month accelerator programme at one of its bases in France.

Synerscope

Founded: 2011
Founders: Jan-Kees Buenen and Danny Holten
Shareholders: Mangrove Capital Partners, 5 Park Lane and Tiketitoo
Funding: €5m
Based: Netherlands
Activity: Synerscope is one of a clutch of companies focused on helping insurers make better use of their data. Its chief technology officer, Jorik Blaas, has a background in MRI scanning and equipment used to look beneath layers of paint on old masters’ artwork. The company aims to take the growing volumes of data that insurers collect — such as data produced by in-car cameras and drones — and turn them into something insurers can use. It has had some success in its home market, with insurers including Delta Lloyd and Achmea using its systems. Achmea used Synerscope to find out which road junctions had more accidents than others. That information can be used not only to reduce claims but also to prevent accidents.

Trov

Founded: 2012
Founders: Scott Walchek
Shareholders: OAK HC/FT, Anthemis Group, Guidewire and Suncorp Group
Funding: $46m
Based: US
Activity: Trov is another company aiming to break insurance down into easily digestible chunks. It sells item-by-item insurance policies for personal possessions, for whatever duration customers choose, via an app. Trov also hopes to improve the claims experience, using a chat service to automate the process. Despite being based in the US, its first market was Australia, where the service has been most popular with 18- to 34-year-olds. Like other start-ups, Trov does not do underwriting itself, preferring to partner with established companies. In Australia, where it launched in May, Suncorp is the underwriter. In the UK Trov’s imminent launch will be Axa, while in the US — where it plans to launch next year — Munich Re will provide the underwriting, it announced in September. *Oliver Ralph*

Investors view insurance as staid and ripe for disruption

Funding

Start-ups are attracting a wide range of backers, writes *Oliver Ralph*

As fast as entrepreneurs have been coming up with insurtech ideas, investors have been rushing to fund them.

Much of the backing is coming from traditional venture capitalists who see insurance — with its large, well-established incumbents and well-worn products — as fertile territory for disruption.

“There have been more investors in the past year than there have in previous years,” says Matthew Wong of CB Insights, which analyses start-up fundraising. “You are seeing investors that have entered the VC ecosystem that weren’t around a few years ago. There are also fintech-focused investors such as Nyca Partners.”

The other big source of funding for start-ups is large insurance companies. “Quite a few of them are forming venture arms,” says Mr Wong. “Some of them see it as a financial opportunity but a lot are looking for strategic benefits. They are also investing in complementary technology such as connected devices.”

By investing in start-ups, insurers hope to have an early look at technology that could change the industry, while getting the opportunity to experiment with new products or services. By owning a stake in the start-ups, insurers also put themselves in a strong position to make an offer for any companies they see as particularly promising.

Among the big US insurers that have established venture arms are MassMutual, Transamerica and American Family, while the big non-US names with venture arms include Axa, Allianz, XL and China’s Ping An.

They have been busy in 2016. According to CB Insights, insurers made 27 investments in 2014 and 61 in 2015. This year they are on track to push that to 79. They are also getting more daring. While investments two years ago were fairly evenly split between early and late-stage funding rounds, this year the early stages have dominated. CB Insights points out that insurers have been particularly enthusiastic investors in companies developing technology for connected devices.

Contributors

Oliver Ralph
Insurance correspondent

Maija Palmer
Digital and communities editor, Special Reports

Bradley Gerrard
News editor, Investors Chronicle

Angus Batey
Freelance journalist

Owen Walker
Commissioning editor
Steven Bird
Designer
Alan Knox
Picture editor

For advertising details, contact:
Peter Cammidge, +44 (0) 20 7775 6321, peter.cammidge@ft.com, or your usual FT representative.

All editorial content in this report is produced by the FT. Our advertisers have no influence over or prior sight of the articles.

All FT Reports are available at:
ft.com/reports
Follow us on Twitter @ftreports