OPERATED BY **FINTNEWS**.COM

THE FINTECH TIMES

| THE WORLD'S FINTECH NEWSPAPER | THEFINTECHTIMES.COM | #13 | JUNE 2017 | £2

Blockhain in Practice | **Top startups to change the World** | **AI queen**

Cyberwars will change the world forever

The world will no longer be the same. The rise of terrorism, which goes hand-in-hand with cyber-terrorism puts a huge question mark over the national security of states and nations. Cyberwars have given birth to a new global security movement, which aims to create a safe cyberspace environment around the world.

In the official speech responding to the London Bridge terror attack, British Prime Minister Theresa May has said: "We need to work with allied democratic governments... to regulate cyberspace so as to prevent the spread of extremist and terrorism planning."

Mrs May's announcement effectively opens a 'fresh page' in the cyber-security field. Existing standards and their regulatory framework will be entirely overhauled, with the market for services and solutions given new stimulus for development. Cyber-security will become Priority Number One at every level – from the computer systems of government agencies through to the domestic appliances in the growing market for 'smart homes'.

Continued on page 3.

HSBC to launch personalised online investment advice

● HSBC is set to launch a new personalised online advice service which will make wealth management advice available at a fraction of the cost to those with a small amount to invest, the bank announced today.

HSBC's Online Investment Advice will use data and algorithms to deliver tailored advice and will make personal recommendations based on an individual's unique circumstances. The roll out will mark the bank's entry into the 'robo-advice' market, which is expected to be available by the end of the year.

HSBC customers with a small amount to invest will be eligible to use the service, simply by logging on via a desktop, laptop or smartphone. On day one, an algorithm that sits in the background will identify a customers' financial circumstances, work out their needs and will then recommend a portfolio to meet these needs.

Brits welcome tech innovations: robot tour guides, driverless car lanes and lunch delivery drones

VIPR launches innovative IBA system to ease distribution cost difficulties

● As pioneers of modern software solutions for the insurance industry, VIPR has launched abrand-new offering to the market. The Insurance Broking Accounts (IBA) system, has been designed to efficiently manage distribution costs amongst stakeholders, alleviating pressures in the industry and resulting in supremely accurate data and payments to cover holders and third parties. Working with leading IBA experts and super-users, VIPR analysed the best of the best in the current market to improve, adapt and modernise key features, creating a system which reaches new heights of software sophistication. Through hyper-efficient data collection,collation, reporting and advanced functionality, VIPR's IBA system can handle high volumes of bordereaux transactions, managing data quickly and accurately. Funds are calculatedand distributed, ensuring the correct payments are made to the right people."

BRITS WELCOME TECH INNOVATIONS THAT COULD TRANSFORM CITIES OVER THE NEXT 20 YEARS

Dedicated road lanes for driverless cars, lunch delivery drones, augmented reality advertising billboards and robotic tour guides are just some of the technologies that could transform cities within the next 20 years according to a survey of more than 2,000 UK adults released ahead of London Tech Week 2017.

Technology will play a major role in transforming global cities, with the research showing that two thirds of people (67 per cent) believe that advances in driverless car technology could lead to dedicated road lanes for autonomous vehicles and more than a third (34 per cent) say they would be willing to make a journey in an un-manned drone taxi. Almost a quarter of people (23 per cent) expect cities to ban human drivers completely.

Consumer adoption rates for technologies that do not yet exist were mixed with the survey revealing that almost half of Britons would be willing to travel at speeds of over 600mph on a high-speed train, such as Elon's Musk's Hyperloop project. Over a third of respondents were also enthusiastic at taking a commercial space flight or commuting to work in a driverless car.

There was less appetite for dining at a restaurant serving a 3D printed meal or purchasing an underwater home. Four per cent of women would be willing to go on a date with a human like robot, compared to twelve per cent of men.

The survey, which was commissioned by the founders of London Tech Week and inspired by a series of predictions put forward by Imperial College London's Tech Foresight group, reveals the technologies consumers think could change our global cities, disrupt traditional industries and drive forward the growth of London's tech sector.

The research also shows that:

- 77 per cent believe we will see eye tracking used to navigate mobile phone applications
- 64 per cent believe there will be solar-powered park benches to charge electronic devices
- 53 per cent believe that tourists will be accompanied by robotic tour guides
- 49 per cent think smart advertising billboards will feature augmented reality
- 47 per cent think DNA dating agencies will be commonplace
- 42 per cent think we will see hangover free alcohol substitutes
- 30 per cent believe high-speed pedestrian walkways will link skyscrapers
- 14 per cent believe there will be underwater housing
- 12 per cent believe flying cars will be commonplace

London Tech Week (12-16th June) is Europe's largest festival of technology, and last year welcomed over 40,000 delegates at more than 300 separate events. Across the week, the festival will showcase the very latest innovations including drones, autonomous vehicles, artificial intelligence and robotics. More information about the event - on the website **londontechweek.com**

THE FINTECH TIMES

- To identify Social, Economic, Political, and Cultural problems
- To explore potential tech enabled solutions
- To bring stakeholders together to develop those solutions

The Fintech Times

Published by Disrupts Media Limited
10 Finsbury Square, London EC2A 1AF
thefintechtimes.com

Editors:
Kate Goldfinch
Katia Lang
Bird Lovegod

Designer:
Monika Zec

Images:
pixabay.com; pexels.com; LinkedIn

No More Ransom!

WannaCry raises Cyber Security to a global priority

Recent ransomware attacks in the UK and around the world have elevated cybersecurity to the top of the international agenda - in areas ranging from politics to national defence, and from smart-homes to global economic systems. How can we buttress our office technologies in today's digital world against the next malicious malware onslaught?

Kate GOLDFINCH

Editor of The Fintech Times

A month ago, on May 12th, WannaCry ransom-demanding malware struck Britain's National Health Service; large Spanish corporation such as Telefónica; and computers across Russia, Ukraine and Taiwan, with hardware and data frozen up and held to ransom.

The coordinated attack managed to cross-infect large numbers of computers across Britain's state monopoly health service in just six hours, partly due to its ability to spread within networks from PC to PC. The ransomware has already caused hospitals across England to divert emergency patients. Global flight delays and other drastic consequences also were monitored.

"Ransomware isn't new, but it's increasingly popular and profitable. The concept is simple. Your computer gets infected with a virus that encrypts your files until you pay a ransom. It's extortion taken to a networked extreme. The criminals provide step-by-step instructions on how to pay, sometimes even offering a help line for victims unsure how to buy bitcoin. The price is designed to be cheap enough for people to pay instead of giving up: a few hundred dollars in many cases. Those who design these systems know their market, and it's a profitable one," explains **Bruce Schneier, Chief Technology Officer of IBM Resilient - a Fellow at Harvard's Berkman Center, and a board member of EFF**.

"The next such ransomware attacks will be worse than WannaCry. We'll need new security standards when hackers go after the Internet of Things," he believes.

The lessons this case brings for users are to keep your system patches up to date, and regularly backup your data. "This isn't just good advice to defend against ransomware, but good advice in general. Yet it's still becoming obsolete."

Cybersecurity as mainstream

The World Economic Forum defined 2017 as the year Cyber Security goes mainstream. "It shouldn't surprise us that the World Economic Forum pointed to this issue. We've already seen some very significant activity this year - be it the recent ransomware attacks or the influence over elections globally. Typically, securing computers and information had been primarily a concern that was discussed mostly by technologists. What we're seeing now is people outside the tech industry being profoundly hit by the results of this topic. I'd suggest their assertions are spot on,"commented **James Chappell, CTO and Co-Founder of Digital Shadows**.

46%
of companies suffered from a cyber attack or breach of their computer systems last year (2016) compared with just 24% the year before (2015).

"Cyber Security has been mainstream for years. If you think back to Y2K or the dot-com bubble, Cyber Security was at the heart of identifying the turn-of-millennium issues, offering solutions to fix them. It only needs major events to occur to bring these issues back into the headlines. There's no denying the ever-critical role Cyber Security plays in today's society," says **Simon Gilbert, Managing Director and Founder at Elmore Insurance Brokers Limited**.

Andersen Cheng, CEO of Post-Quantum focuses on the opposite: "It's troubling that such definitions [as the WEF's] are still necessary. Cyber Security is a central facet of our time, affecting everything from business operations to our personal lives – and increasingly the overlap between these areas. Protecting your data, both as an individual and as part of an organisation, is fundamental nowadays. We need to go beyond abstract terms like 'Cyber Security' and prioritise aspects that people can engage with and do something about - protecting their information and their identity at home, and at work. We also need to help people understand the value of that data – why someone might want to steal it, and the effect losing it could have".

Moderating discussion around the "Cyber Security mainstream thesis", it is very sanguine to note that 46% of companies suffered from a cyber attack or breach of their computer systems last year (2016) – as compared with just 24% the year before (2015). The risk of cyber attack doubles each year.

Leading global analytical centres, consultancy firms and experts have fallen in line with the "mainstream conclusions" of Cyber Security trends-2017.

- As an example, **Symantec** predicts "the enterprise network will expand, to become increasingly undefined and diffuse - ransomware will attack the Cloud and fileless malware will increase". McAfee covers a wide range of trends and 2017 predictions worth noting. Among these are the following: "Ransomware will remain a very significant threat until the second half of 2017. Ransomware-as-a-service, custom ransomware for sale in dark markets, and creative derivatives from open source ransomware code will keep the security industry busy through the first half of the year. Ransomware's impact across all sectors and geographies will force the security industry to take decisive action. We predict that initiatives like the No More Ransom! collaboration, the development and release of anti-ransomware technologies, and continued law enforcement actions will reduce the volume and effectiveness of ransomware attacks by the end of 2017".
- **Forcepoint** highlights: "Compliance & Data Protection Convergence - 2017 will be the final full year before the European Union's (EU) General Data Protection Regulation (GDPR) becomes a legal requirement. GDPR demands may drive business costs higher as new data protection controls are applied, and multiple stakeholders grapple with the Who, When and How of data accessibility requirements".
- **FireEye** offers a slightly different approach: "In 2017, Cyber Security battles may favor criminals even more - as the Internet of Things (IoT) continues to expand possible avenues of attack. Security integration and orchestration should be considered the benchmarks of new technology investment."
- **Kaspersky Labs** predict that 2017 will continue to see the commodification of financial attacks. "The commodification of attacks along the lines of the 2016 SWIFT heists — with specialised resources being offered for sale in underground forums or through as-a-service schemes, will continue in 2017. As payment systems become increasingly popular and common, this will be matched by a greater criminal interest next year. As far as ransomware is concerned, Kaspersky Labs also anticipates the continuing rise of ransomware - but with the unlikely trust relationship between the victim and their attacker, and based on an assumption that payment will result in the return of data."

"We need to adapt to a world that is changing due to data explosion, an increasing number of cyber-threats, a need for fast and secure access to data, and also new regulations," Jérôme Totel, Vice President Product & Sales Engineering, at DATA4 GROUP, concludes.

"The main challenges we are facing right now are fast moving targets, a lack of skilled people, a need of intense collaboration and a regulatory framework which will increase in complexity.

Continued on page 4 ▸

Continue from the previous page

Cyber Security needs a transverse and cross-sector approach. It as a collective challenge," underlines **François Thill, Assistant Director Communications, Ministry of the Economy and Foreign Trade Luxembourg**.

Oliver Saban, project director of Fintech1010, highlighted the same thesis: "Organisations and government need to collaborate so a common message and framework is filtered down to the retail level. Financial organisations potentially need more assistance as they are the custodians of the individual and insurers are a part of this process."

Overwhelmingly, Michael Hofmann, CEO, KPMG Services, lists the following key Cyber Security trends: external threats, change in the way business is conducted, rapid technology change, regulatory compliance and changing market and client need.

The regulatory framework

The National Cyber Security Centre (hereinafter NCSC) is a key means for government to deliver many elements of strengthened Cyber Security for the UK.

Britain is being hit by dozens of cyber-attacks a month, says **Ciaran Martin, head of the new NCSC**. As an example, the Centre has blocked 34,550 'potential attacks' on government departments and members of the public in the past six months – about 200 cases a day. Martin confirms, that Britain had been hit by 188 high-level attacks, "many of which threatened national security", in the last three months. "In the case of government departments, [it involves] getting into the system to extract information on UK government policy on anything from energy to diplomacy to information on a particular sector."

Philip Hammond - a former Defence and Foreign Secretary, warns that hacks could bring down national infrastructure and that even kettle, fridges and driverless cars are at risk. He stresses that the 'internet revolution' has brought the threat of being held to ransom by hackers, the theft of intellectual property and the "shutting down of critical national infrastructure".

"Beyond hacked kettles and fridges, 'Internet of Things' devices, such as driverless cars, can present alarmingly real security threats that could be incredibly dangerous if the right security isn't in place," Hammond adds.

The 2015 National Security Strategy (NSS) reaffirmed cyber threats as one of the most significant risks to UK interests. The NSS set out the Government's determination to address cyber threats and put tough and innovative measures in place as befits a world leader in cyber security. To deliver on that commitment, on 1st November 2016 the Government published the 2016-2021 National Cyber Security Strategy, in which it was committed to invest £1.9B.

What is National Cyber Security Strategy mostly concerned with - protecting the government, or protecting the UK's digital economy?

"We directly benefited from the first grants in 2015. We saw this recent commitment very much to protect the UK economy which in turn helps strengthen the government and its supply chain," **Simon Gilbert, Managing Director and Founder at Elmore Insurance Brokers Limited, specialists in cyber-insurance**, says.

"This is about both. In order to protect the UK economy and government, we need an effective commercial Cyber Security industry. The UK is in a unique position in that, we have a strong heritage in encryption, engineering and computers combined with an internationally recognised education sector. This is a fantastic position to grow and inspire strong capable companies who can offer services to secure the UK economy and Government. The investment announced by the chancellor in November last year is in part about creating world leading support such as that in the National Cyber Security Centre (NCSC) and critically support from the Department of Culture, Media and Sport in creating and inspiring a new generation of Cyber Security startups who become the companies to lead the industry of tomorrow. There is a genuine opportunity to create a strong sovereign Cyber Security sector in the UK which can lead global innovation in Cyber Security," argues **James Chappell, CTO and Co-Founder of Digital Shadows**.

Meanwhile **Oliver Saban, project director of Fintech1010**, supports the point of view that NCSC protects both sides and raises awareness. "Initiatives can be put into place to raise awareness and simple security measures can be implemented to mitigate initial threats."

Cyber Security functions

It's difficult to come up with a one-size-fits-all approach, but broadly speaking most Cyber Security strategies should consider the following, **James Chappell believes**:

- **Basic cyber hygiene** such as patching systems, using secure passwords, creating cyber aware organizations that report incidents.
- **A risk-led approach**, which properly understands the digital risks to organisations, and determines approaches to put in place as mitigating controls.
- **Effective monitoring** on computer networks and reporting points for people to spot when an attack might be happening, or when accidents occur.
- It is critical to create some kind of **incident response and recovery capabilities**, which helps organisations in effective response and recovery from incidents. This should involve the whole organisation, including the PR and senior management teams. Ensured resilience is critical for organisations.
- **Creating secure cultures**, where people understand that security is everyone's responsibility and create 'situation awareness'
- **A compliance approach**, helping organisations to demonstrate they are meeting their legal, regulatory and commercially-required commitments.

"Generally we see the functions ranging from services, software, hardware and physical security then a combination of those. Breaking these into sub-sections of different services creates a picture of a hugely diverse and complex industry," **Simon Gilbert** describes.

Cyber Security solutions tend to target three customer segments - individuals, organisations and government. Let's analyse which segments require more Cyber Security solutions so far? "I don't think any one requires more than the other, they are all part of the same global connected problem. A bank has customers with unsecured endpoints has to consider both ends of this. Governments that have to ensure the resilience of the economy require businesses and their users to be secure," **James Chappell** notes.

"The customer changes, but across these the vulnerability and the solution are often the same: people are at the centre of Cyber Security. At Post-Quantum, we design our systems to help people operate more securely by removing single points of failure – those points where someone's level of access can be exploited, by an attacker or of their own desire. We do this by using biometrics to reduce reliance on passwords, and by cutting the effectiveness of phishing and whaling attacks by only giving access to high-value data and systems if multiple people agree to grant that access," **Andersen Cheng** explains.

How should SMEs protect their businesses

The sophistication of the threat has increased. As a result, "organisations are progressing their approaches to security," **James Chappell explains**.

SMEs need to consider their security from both a people and a technology perspective.

"Thinking first about their people, we recommend using biometrics for ease of use when accessing systems and sensitive data to help employees be more secure in their activities. We also suggest implementing multi-party authorisation to access high-value data and systems, to remove single points of failure and reduce risk," **Andersen Cheng, CEO of Post-Quantum** notes. "On the technical side, businesses need to ensure they have cryptographic agility in their systems. As new weaknesses in encryption schemes emerge – whether that's the result of increased computing such as quantum computing or an underlying vulnerability in the cryptosystem – businesses cannot be in a position where they're tied to a particular encryption algorithm and unable to switch to something else should that be broken."

A great place to start your business protection is the Cyber Essentials framework provided by the UK government, **James Chappell** advices.

As for **Simon Gilbert, Managing Director and Founder at Elmore Insurance Brokers Limited**, specialist in cyber-insurance, it is very important to train employees, get cyber essentials, back-up company data, regularly update software, create a data asset risk register, and know who you are going to call when things go wrong.

Oliver Saban, project director of Fintech1010, also supports this point of view. "You need to understand the market and to seek consultancy firms for education."

Threats and opportunities

Experts predict Cyber Security will play a crucial role in global politics, although in a more overt manner than in previous years. "The role of social

media in our democracies will continue to be a battleground. With the release of government grade vulnerabilities in computer systems we will see the organised criminals exploit these techniques and tradecraft to maximum effect. Governments outside of the traditional nuclear states will invest in their own capabilities to both defend and invest in their global political interests abroad," **James Chappell** has no doubt.

Some disruptive technologies (such as blockchain), integrated into Cyber Security eco-systems, could be considered as both opportunities and threats simultaneously. "This year we're seeing a great many blockchain projects underway, and large organisations are starting to consider that the technology offers a new business stream. or is a replacement for legacy systems. This, however, creates a significant Cyber Security threat. The cryptographic signature scheme which underpins blockchain is known to be vulnerable to attacks by quantum computers. By implementing 'standard' blockchain technology, businesses are storing up risk and expense for the future. The deployment time for a large-scale enterprise blockchain implementations will nearly overlap with the advent of code-breaking quantum computers - making the business' new system vulnerable almost immediately. There is an opportunity now to future-proof these deployments with quantum-resistant signature schemes. This will save time and costs by eliminating the need to migrate again soon after the system is in place," **the CEO of Post-Quantum** adds.●

COMMENTS How would you evaluate existing Cyber Security standards and their effectiveness - and what can be improved or redesigned (globally and in the UK)?

James Chappell

CTO and Co-Founder of Digital Shadows

One of the beauties of standards is that there are so many to choose from. Cyber Security as it is today, grew from the closely related topics of information assurance and computer, information and network security. The truth is that standards have existed for some time that help organisations measure, quantify and manage risk. BS7799 was one of the first approaches to this, and since that time we've seen many new frameworks such as the US Cyber Security Framework, COBIT, ISO27001:2013 and Cyber Security assurance frameworks such as Cyber Essentials. The size of your organisation, the types of critical business functions it engages in, and the industry sector can make affect your selection in making the best pick.. Yet the principles behind them remain similar. Figure out what you have to protect, work out what the threats are to them, prioritise the best places to focus your protection efforts - and then deploy effective measures and measure their effectiveness.

Andersen Cheng

CEO of Post-Quantum

The greatest challenge for the effectiveness of Cyber Security standards will be the emergence of quantum computing. In the near future, this will render most encryption currently in use ineffective. NIST in the US is taking steps to find encryption algorithms that can succeed today's standards. Even so, the threat is poorly understood by business. Many leaders still see this as something that will not affect them in their tenure - yet data stolen today could be accessed in the future. This has serious implications for organisations with high-value data, and they must ask themselves what data they hold that would affect their bottom line if it were accessed in 5+ years time. They then need to pursue a policy of cryptographic agility - to prepare their systems and give themselves the flexibility necessary to meet this challenge.

Oliver Saban

Project director of Fintech1010

In December 2015 two pieces of EU regulation were agreed - the General Data Protection Regulation (GDPR) and Network and Information Security (NISD). Both shift the balance of power towards the citizen to whom the data belongs - and away from the organisations that analyse and use such data. They have been designed to create focus on the protection of IT systems in European critical infrastructure. These new regulations will affect all sectors, most notably the Financial sector.

Starting in 2016, there will be a two year period during which organisations will be allowed to prepare for the new regulations and for the Directive to pass into membership law. It should now be understood, that existing Cyber Security standards are in motion to support and accomplish a common framework to which groups should adhere. Responsibility is on individual businesses to realise that this framework is now moving towards support the security of the client - and without knowledge of these Directives, or a conscious drive towards a common framework, groups may be put at risk. Those risks are equal, whether they mean falling short of the Directives, or having inadequate systems in place to protect clients from Cyber Security attacks.

CYBERSECURITY AND INSURANCE

FICO Survey: Nearly One-Third of UK Firms Don't Have Cyber-Security Insurance

The General Data Protection Regulation (GDPR) requirements - the biggest change to EU privacy law – which come into force in the UK on 25th May 2018, introduce higher fines for cases of data breach. Even if ransomware attacks don't increase in volume, they still make having comprehensive insurance more important. Companies with stronger cybersecurity strategies and data protection could expect to pay less for cybersecurity risk insurance.

The consultancy firm Ovum, conducted a survey for Silicon Valley analytics firm FICO by holding telephone interviews with 350 CEOs and senior security officers based in the US, Canada, the UK and the Nordics in March and April 2017. Respondents represented firms in financial services, telecommunications, retail, e-commerce and media service providers.

UK firms are increasingly protecting themselves with cybersecurity risk insurance, but nearly a third of firms have not taken out insurance yet. The survey reveals that even among those that have insurance, only 28 percent said they have cybersecurity insurance that covers all risks.

Even though the majority of firms surveyed have cybersecurity insurance, most say that the risk assessment process insurers use needs improvement. Just 31 percent of respondents think their premiums reflect an accurate assessment of their risk. Nearly as many - 29 percent - said they don't believe the assessment accurately reflects their risk, and 11 percent said they don't know how their insurance is priced.

The survey highlights:

- 31 percent of UK executives surveyed say their firm has no cybersecurity insurance, compared to 40 percent in other countries surveyed.
- Only 28 percent of UK firms surveyed have cybersecurity insurance that covers all risks.
- 69 percent of respondents say insurers should do more to explain how they price risk.

"The UK will soon be subject to General Data Protection Regulation (GDPR), which introduces higher fines in cases of data breach," said Steve Hadaway, FICO general manager for Europe, the Middle East and Africa. "Even if attacks don't increase in volume, firms could end up paying more, which makes having comprehensive insurance more important. At the same time, companies have a right to expect that they will pay less if their protection is better. The onus is on the cybersecurity insurance industry to make sure insurance rates are fairly set for each individual firm, based on a sound analysis of its risk."

As a response to the above-mentioned, the quote of **Martin Overton, EMEA Cyber Risk Specialist, AIG,** can be provided: "Since introducing cyber liability insurance in 1999, we have helped thousands of companies and more than twenty million individuals respond to a cyberattack. In order to prevent themselves from cyber threats, insurance companies are working with customers to help them improve their security maturity via partner services, consultancy and learning from others' mistakes and failure."

OPINION Cyber Insurers WannaCry

The ultimate test for Cyber Insurance

Cyber Insurers and Brokers alike will remember Friday 12th May 2017 as a potentially a catastrophic global cyber-attack with the ability to bring a claim under every single cyber insurance policy, all at the same time! This was unprecedented and fortunately had it not been for a UK security consultant accidently deploying a kill switch the damage could have been far worse.

If you haven't already, update all windows software as soon as possible and if you are running anything less than Windows 10, update your Windows using the special Microsoft patch here. Do a AV and Malware scan of your network, back-up your data and give everyone in your company a phishing lecture.

WannaCry unleashed itself onto the world, as terrorist attacks do, indiscriminately, with no notice and with lethal force, it is not surprising that sophisticated hacker tools are commonly being referred to weapons of mass destruction.

This time is different

We are all too familiar with mega data breaches, where tens, if not hundreds of millions (and in AOL's case billions) of individual's sensitive information being compromised. But it generally passes people's attention as just another data breach. So why is WannaCry different? Firstly, this was not a hack of any particular company or system but rather the use of a highly sophisticated NSA cyber weapon which has been entwined into a form of malware called ransomware. Secondly, the scale of the phishing attack in just 72 hours, crossed 150 countries and (Europol predicts) some 200,000 systems impacted and if the second version of the ransomware is released another 1,000,000 systems could be exposed. To add further fuel to the disruption, the ransomware self-replicates, which means when one computer is infected it will unilaterally infect other computers in the network.

Normally a hack leads to data loss, and not to physical damage or injury. However, in this case, one of the worst impacted entities of the ransomware has been the poorly funded NHS. It is rare to consider the UK's Computer Misuse Act 1990 (rather than the Data Protection Act 1998) when thinking of cyber-attacks, but in the UK, a person guilty of causing physical injury through cyber-attack can be imprisoned for life under the 1990 Act. With almost 40 NHS Trusts on their knees, over a usually busy weekend, the chances of serious injury occurring from the attack was greatly increased. Reports of operations, appointments and ambulances being cancelled, doctors being unable to access patient data and potentially life threatening circumstances being made even more severe, the consequences of the attack were far and wide ranging.

What could WannaCry cost Cyber Insurers?

This is where insurers start to panic, how far and how wide does this event effect them and what parts of a cyber insurance policy could be claimed under? The only positives for cyber insurers, at this stage, is that a kill switch was deployed before the attack could reach the US and Canadian markets and cyber insurance is in its relative infancy outside of these markets, and therefore still in the early days of adoption (where some two thirds of business purchase). It is expected only 10% of UK businesses purchases cyber insurance, but that number is rapidly increasing. However, any positive insurers can draw from that, will quickly disappear when reminded of the scale and extent of this attack. Every cyber insurance policy issued could bring a claim against it should the policyholder have received and clicked on the ransomware email. It appears from stories leaked to the press so far that only $50,000 in Bitcoin has been paid to criminals, however it is not the ransoms which could be potentially crippling for cyber insurers, but the business interruption and increased costs of working.

It is the lost revenues and the costs to get systems up and running again which can cause the biggest losses to businesses impacted by such an attack. In the US, where developed data protection regulation is in place, business mostly purchase cyber/privacy liability protection and often don't purchase the business interruption element of the coverage. However, in Europe, Middle East and Asia, cyber insurers for some time have been offering comprehensive business interruption caused by cyber-attack in light of the relatively benign regulatory environment, and as such almost every policy has this coverage included.

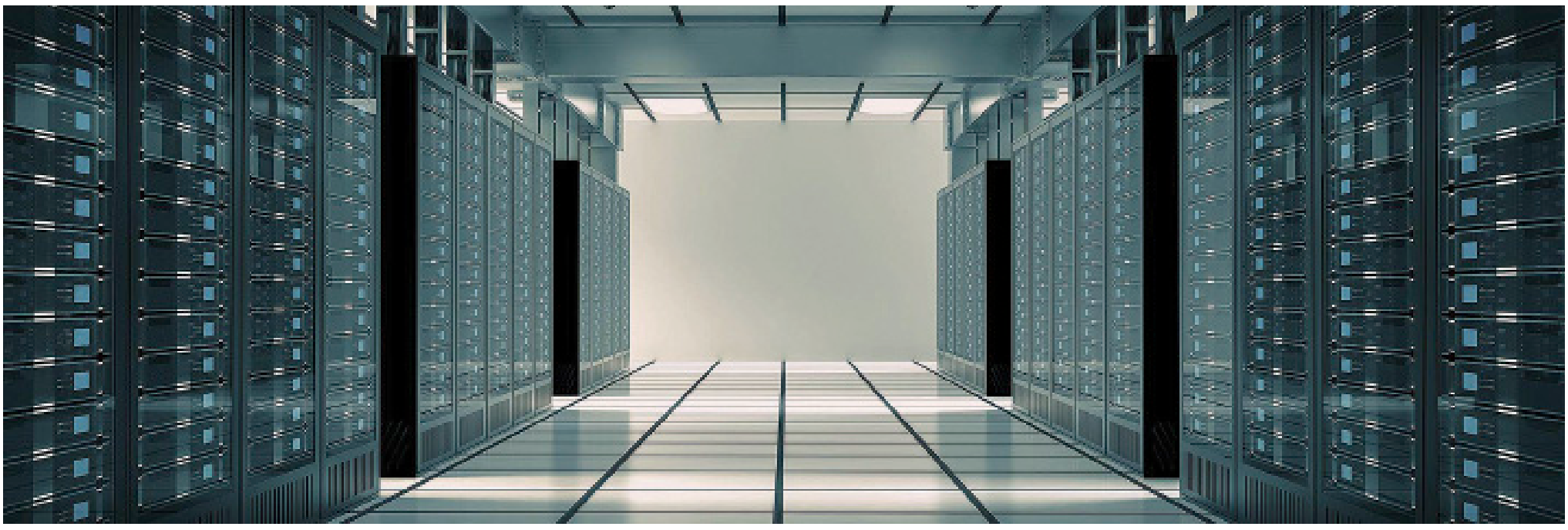
The potential increased costs in working and delays caused by WannaCry could cost businesses around the world hundreds if not billions of dollars. An example of this, is one particular NHS Trust impacted by the attack had 2,000 of its 6,000 PC's infected. Of these 2,000 PC's there is a choice either to pay the ransom or wipe them. In some cases, it may be quicker (and safer) to purchase new PC's than try and bring back infected PC into commission. Just this organisation alone, had it been buying cyber insurance, could be seeking a claim for millions of pounds. Multiply these numbers by the potential of millions of companies around the globe being impacted by the attack and the cost to insurers could run in to the billions.

What happens next?

There are going to be more attacks, wider reaching, more sophisticated, and potentially much more damaging. Cyber risk is moving from the digital world to a physical reality. Already there are examples of significant physical damage caused by cyber-attack (such as the replacement of 50,000 computers for Saudi Aramco or the explosion at the steel mill in Germany) and this causes a real headache for insurers and policyholders alike. Cyber Insurers will be considering their exposures in managing future attacks and policyholders need to understand whether they have suitable protection.

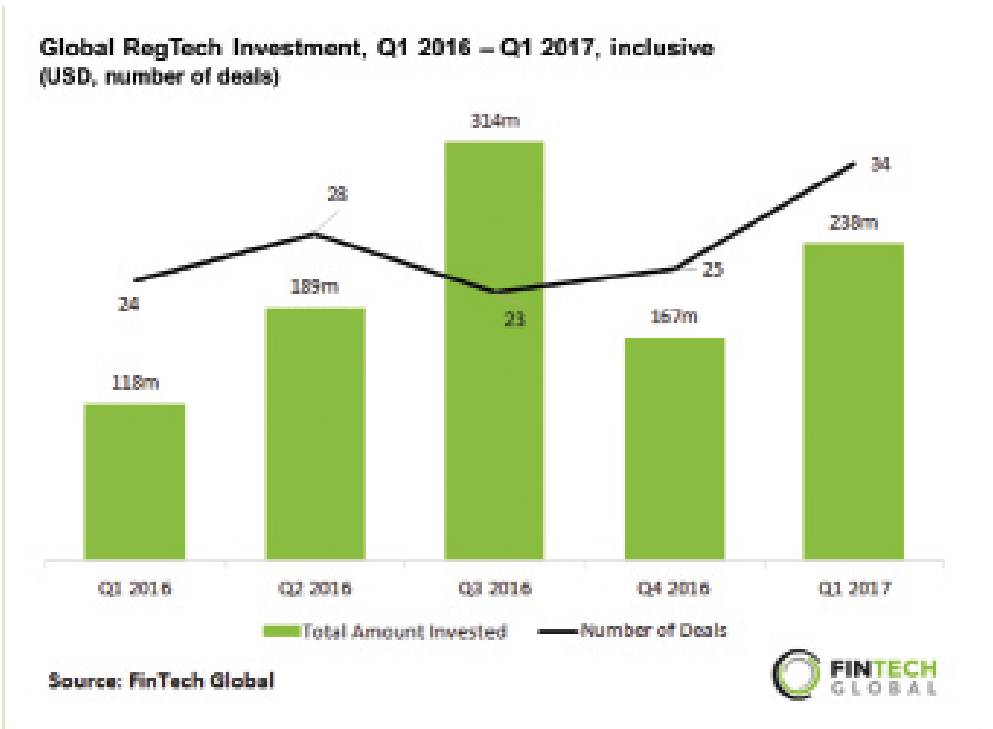
We advise businesses to review their insurance policies to ensure sufficient coverage is in place, particularly regarding the coverage around ransom, extortion, business interruption and reputational harm. If you are not sure we recommend having a Silent Review which acts as a health check of existing insurance arrangements.

Simon Gilbert
Managing Director and Founder at Elmore Insurance Brokers Limited, specialists in cyber insurance



RegTech deals surge to record levels in the first quarter of 2017

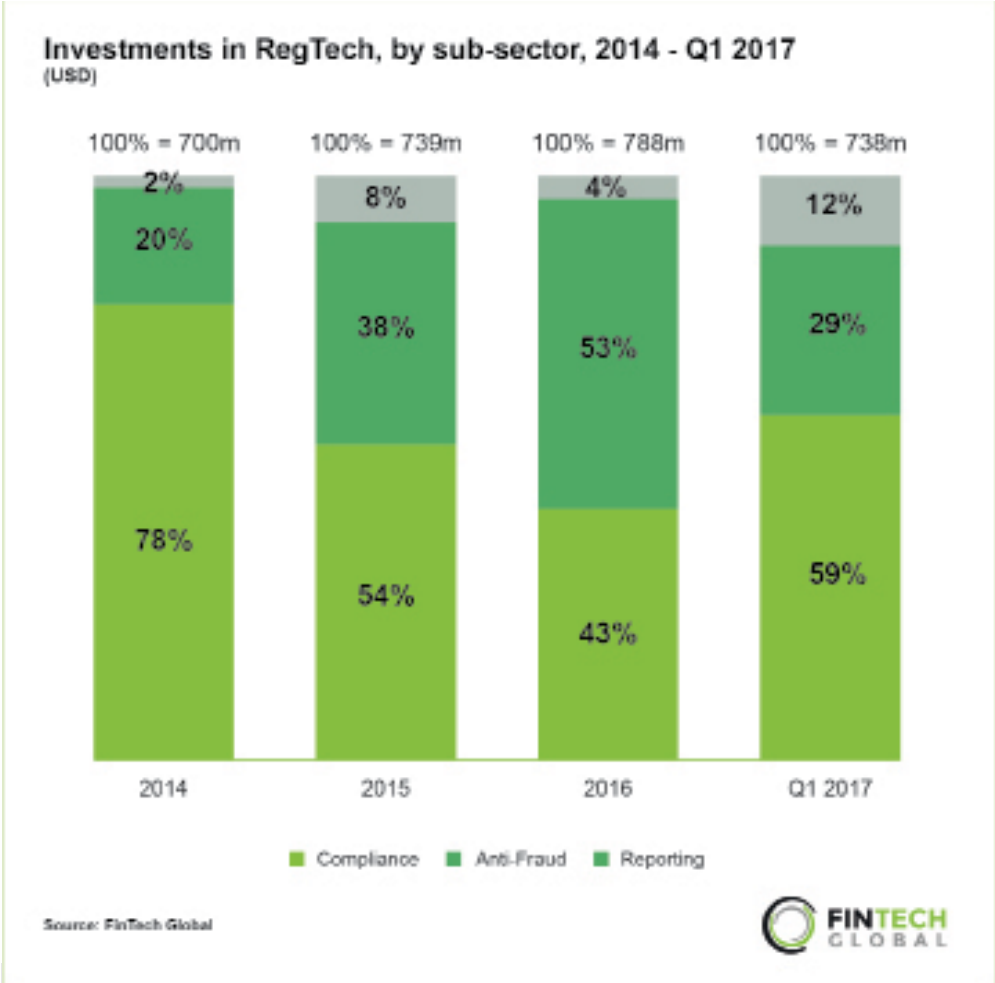
THE NUMBER OF INVESTMENTS MADE IN REGTECH COMPANIES MORE THAN DOUBLED IN THE FIRST QUARTER OF 2017, ACCORDING TO RESEARCH FROM FINTECH GLOBAL.



RegTech companies raised a combined total of $238m across 34 deals, a record number of transactions, in the opening quarter of 2017. Total funds raised by the sector grew 102% Q1-on-Q1 although the total remained below the peak reached in Q3 2016 when $314m was committed to RegTech companies. The largest deal involved Netwrix, an Irvine-based compliance startup, which raised a $51m Series A round from Updata Partners in February of this year.

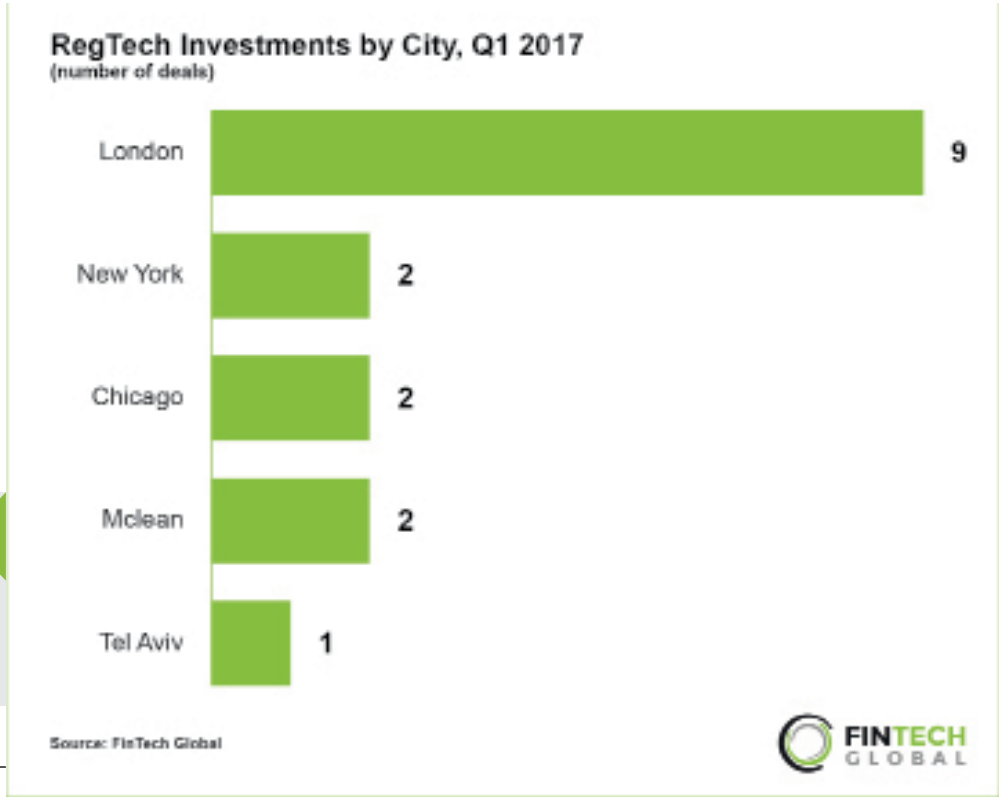
London maintained its dominance in Q1, closing nine deals, the largest of which was the $12.5m Series B Round raised by Dealflo, a financial agreement automation service. Unsurprisingly, the increase in investments in RegTech is accompanied by excitement about the subsector's future prospects. It would be no surprise to most investors if 2017 turns out to be a record year.

INVESTMENT IN COMPLIANCE-FOCUSED COMPANIES MADE A COMEBACK IN Q1 2017



An analysis of deals by subsector shows that compliance-focused investments staged a comeback in the first quarter of the year raking in 59% of RegTech investments, outstripping funding to anti-fraud companies which took in the largest share last year. The share of investments taken by companies in the 'reporting' subsector saw an uptick in Q1, rising to 12% from only 4% of total RegTech funding in 2016.

LONDON CONTINUES TO CLOSE MORE REGTECH DEALS THAN ANY OTHER CITY



Fast-forwarding RegTech Adoption: the Case for Industry Sandbox

Industry Sandboxes could be effective pan-industry platforms that support the development, validation and adoption of RegTech solutions in financial services.

An Industry Sandbox is as a collaborative digital platform that makes it easier for developers to test a product and prove the viability of an innovative solution using industry data, applications programming interfaces (APIs), and off-the-shelf technology solutions.

Industry Sandboxes would be open for participation from all players in a FinTech ecosystem, including startups, financial institutions, established data and technology vendors, and regulators.

Innovate Finance was invited by the FCA to conduct a consultation of the need for an Industry Sandbox and its potential design.

Pooling feedback from over 200 participants, 30 contributing authors, and a global survey of best practices, the consultation report, published in early May, presents a menu of use cases and design features that would make an effective sandbox of this type.

RegTech adoption was one of these use cases. Why was this raised as an issue in the first place?

Here are four potential challenges in the development of a RegTech solution in the current market environment:

- **Transfer of knowledge:** identifying the painpoint a RegTech company is to address requires detailed knowledge of both financial services and regulation. This knowledge is not always accessible to the entrepreneurs that have the freedom to innovate.

- **Understanding of technological requirements:** RegTech solutions need to integrate seamlessly with the existing operational processes and technologies in multiple institutional clients. These requirements could to be more transparent, and in some instances standardised.

- **The risk of complying through innovation:** RegTech solutions offer new ways to meet regulatory requirements. Innovation, by definition, requires trial and error, which are uncomfortable concepts in compliance. A platform which allows multiple institutions to validate a single RegTech solution at the same time might help overcoming such risk threshold.

- **Regulatory feedback:** RegTech solutions can benefit from curated feedback from the regulator provided as early in the development process as possible. Regulators would participate as observers in an Industry Sandbox and as such as provide feedback to multiple startups who are tackling a similar issues.

Building on these challenges, below is the real-life example of the RegTech company Sybenetix whose Chief Marketing and Strategy Officer, Richard Maton, has developed a use case of an Industry Sandbox.

A view from, Richard Maton, Chief Marketing and Strategy Office, Sybenetix

The framework being developed by the industry for MiFIDII data management and reporting provides the catalyst for innovative technologies such as AI and new collaborative models enabled through the Cloud to transform risk and compliance effectiveness for both firms and regulators.

For example, Sybenetix's Behavioural Analytics Model applies algorithms to individual decision making to provide a holistic behavioural analysis of market abuse, conduct risk and investment performance. Supervised machine learning is used to eliminate false positives for market abuse surveillance, provide instant insight based on individual behavioural profiles, and an evidence-based conduct risk system for senior managers and accountable individuals.

Developed for firms and regulators, the Behavioural Analytics System is validated by a community of leading financial institutions and through the traditional processes and timetables of regulatory scrutiny. Sybenetix is currently working with partners to scale its Behavioural Analytics Model using cloud infrastructure being developed for the granular data reporting required by MiFIDII. The company is also solving new regulatory challenges associated with the use of AI in financial services.

The Industry Sandbox could help accelerate Sybenetix's development process through a faster, more efficient digital collaboration framework that creates new standards for proactive conduct risk management while further reducing costs and risk for both firms and regulators.

Ultimately, the value proposition of the Sandbox for RegTech firms, financial institutions and regulators is its capacity to accelerate off- market testing to on-market use and scaling. The key is designing the right process and testing mechanisms within the Sandbox that all stakeholders can align around to validate new RegTech solutions. For example, defining a standardised set of KPIs for more effective regulatory outcomes of new solutions that link directly to the application of core technologies and business models. This should include an assessment of how new solutions and models reduce operational risk compared with legacy systems and models. For example, how systems scale with the speed, breadth, accuracy and transparency required under new regulations.

The application of this RegTech acceleration framework could extend beyond conduct risk to the broader set of risk and regulatory challenges that RegTech solutions are solving. For example, the development of KYC/AML monitoring, regulation scanning, interpretation, change management, reporting and risk management solutions. Such a framework would enable faster validation of new systems for use by both participants and supervisors. This framework could also help facilitate new collaborative designs of more effective and efficient regulation, such as real-time supervision, and even new models of self-regulation.

Consequently, the Sandbox could also enable regulators to accelerate how they become more 'digital' through a collaborative framework that fits into broader, global policies and mechanisms being developed. For example, integrating an Industry Sandbox with other testing mechanisms such as sprints and sandbox initiatives in other jurisdictions would also benefit Sybenetix, its partners and its global financial institution clients.

industrysandbox.org/case-study/regtech/####

Europe takes on China on mobile payments

By Yelena KENSBORN and James MAYER

Whether or not you think that the future lies in financial technologies, it is hard not to be impressed by the sector's astronomic growth. Rarely have we seen an industry expanding at the rate 'FinTech' did in 2016 when it attracted over $17.4 billion in investment. For the first time ever, China outpaced the U.S. in both the amount of deals completed and the total capital raised by start-ups. During the year, Chinese investments into FinTech companies grew by an astonishing 84%, making the country the market leader in one of the most modern and prominent technology sectors in the world. Meanwhile, the money flowing into western companies dropped dramatically. The U.S. and U.K. saw 12% and 34% decreases in investment respectively while, in Europe, the amount of investment fell from $12.4 billion in 2015 to only $2.2 billion last year.

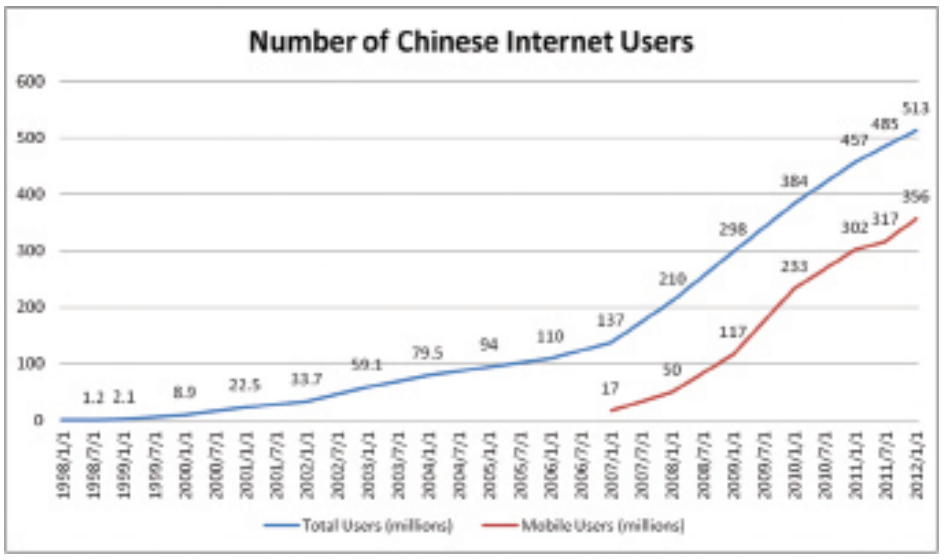
This transformation was, therefore, one of the main discussions at the eFinTech show is Barcelona this year. The event attracted companies from all around Europe. All came to discuss current trends and ways European start-ups could compete on a global scene.

"We've seen a fall of investment because of the political instability" says Fabrizio Villani, founder of Fintastico, a global FinTech portal that features start-ups from all over the world. "At the moment, most FinTech start-ups are targeting the whole [of] Europe. This includes the UK, which, of course, is the biggest market. So, at the moment, FinTech start-ups can expand into other European countries without having to apply for a completely new license each time", says Villani.

But while political instability may be factor that played a big part in this change, it's clearly not the only reason for the shift. Looking at the Chinese and European markets development, it is evident that the journey to the current standpoint looks very different in the two continents. While the western economies are characterised by stable growth with a financial system that gradually adapted to customer needs, China has built their digital market from a very different base. Their enormous economic growth over the past 20 years meant that many consumers went from a cash-only daily life straight to paying for goods and services on their mobile phones, bypassing the plastic bank cards Europeans have been using during the past decades.

As China became the country with the greatest amount of Internet users in the world (over 700m), with the whole population moving onto smartphones almost over night, cash-free payment options were suddenly possible but massively under served. This resulted in a clear competitive advantage for Chinese FinTech companies over their western counter parts, which used the opportunity to make China into the mobile-payment country it is today.

Anyone who's ever been to China would have seen the enormous amounts of QR code scanning



happening and the heard the bleeping sound made by smartphones processing successful transactions. The leading Chinese mobile payment solution, AliPay is, literally, everywhere. Everyone, including beggars in the street, take and makes payments through their phone. As a result, the parent company behind it, Ant Financials, is expanding at the fastest rate in the market and is engaged in acquiring dominant players in the leading economies around the world.

Apart from AliPay's recent acquisitions and investments of major Asian mobile payment companies such as Paytm in India, Ascent Money in Thailand and Kakao Pay in Korea, it now appears that the company might have won the bidding war for MoneyGram, the leading money transfer company in the U.S. This bidding war against the U.S-based company Euronet, seems to have ended after an increase to the bid from the initial offer of $880 million to $1.2 billion. While the bid still needs to be approved by the U.S. committee of Foreign investment, where Euronet might seem to have an advantageous position, Jack Ma AliPay's founder has already discussed the deal in a meeting with President Trump, who will have the final say.

As a result, European FinTech companies are now looking for competitive advantages over their fast-growing Asian counterparts in the global market.

"We really need to think about this. If we don't support and grow the FinTech scene here, how are we going to compete with non-European players if they decide to set up in Europe?" says Fintastico's founder Villani.

Unlike China, Europe does not have a leading mobile payment provider and, while there are many different arguments about the causes for this; the large amount of regulations attached to the operations for running a financial services company, is clearly a factor, that makes it harder to set up and run a financial technology company in the west. The regulations also make it difficult for new companies to penetrate already mature and advanced markets. However, this is about to change, according to IBM FinTech "Thought Leader" and author of "FinTech Innovation" Paolo Sironi. He points out that there are many new regulations that could make Western economies more competitive in the near future. One of these, he says, is PSD2 which, amongst other things, allows for real-time online transactions and better customer protection with FinTech start-ups sevices, that will make the European market more competitive when it comes to mobile payment.

"PSD2 is due to facilitate open banking in European markets by requiring that banks offer data access to third party solutions through API's, conditional to regulatory approval of a trusted license. Easier data sharing will clearly foster frictionless innovation outside the banking club, granting to FinTech a more competitive playing field", says Sironi.

The plan with this regulation is to make it easier for FinTech companies to operate and make it more competitive internationally. It could also make it easier to transfer regular bank customers to digital payments, allowing for expansion of services. These features would, hopefully, make it possible for European FinTech companies to, not only dominate the domestic market, but also expand internationally into markets with a familiar language and culture.

"There's a lot of room for innovation in Latin America. If you go to Columbia, you can end up queuing at a cashpoint for hours, so mobile payment solutions make a lot of sense", says the founder of the Spanish FinTech incubator Innsomnia Francisco Estevan. The incubator works with established banks and links them to start-ups in order to create an effective infrastructure for FinTech innovation. Estevan sees this as a great opportunity for both Spanish and Latin American entrepreneurs to get access to capital and customers, making it possible to implement and test new ideas on the scale of a mass-market.

With major players, banks and financial institutions all competing for the people to use THEIR service, the situation can be described as confusing at best. While the politics and the capital involved in the FinTech startup scene is so large that it's equivalent to many countries' GDP, the word still doesn't make sense to most people outside of the tech industry. FinTech might even seem like a buzzword, one that's likely to drop out of fashion within a few years. One thing, however, is certain - we're witnessing a battle for the next generation customer. Even if the word disappears, the world is changing at a very fast pace and when the storm settles, there is certain to be a new order we are all a part of and that new order will be built on financial technologies.

Could GovTech become bigger than FinTech?

GovTech is gaining momentum as it is passes from an emergent state and is poised to go global. It could be today in a similar investment position as FinTech was 6 years ago. With a global market potential estimated at $500bn it could become bigger than FinTech, according to a report produced by GovTech Research titled "GovTech: an Emergent Sector Revolutionising Public Services"

Ian DOWSON

Co Founder GovTech Research and GovTech Meetup Group London

What is GovTech?

It is the result of a coalescence Government and civic activity with digitalisation. GovTech and CivicTech revolutionise the public arena. CivicTech is usually not for profit services for Citizens while GovTech Startups digitise public and civil services and have a for-profit based model.

Fundamental change

Users and user needs are put at the core of this transformation - be they citizens, government departments or businesses. This requires a complete culture change within government to becoming focused on system and service outcomes not internal focus. The UK Government has made pioneering progress on this front being ranked No 1 in E-Government by the United Nations and No 1 in Open Data by The World Wide Web Foundation.

System wide change powered by Open Data

Process change is not all the UK Government has done, procurement policy is now favouring SME's, and Open Data has become policy for all Government departments, public bodies, cities and local authorities. Examples such as Data.Gov.UK, Transport for London (TfL), London Datastore and DataMill North, illustrate progress made in providing open data. This effort is also supported by civic institutions such as NESTA and ODI (Open Data Institute) and Local Government Association.

Blueprint Emerges

A blueprint for how government and civil society services can undertake digital transformation has emerged, but there is much to be done. Simply the scale of the task of digital transformation is beyond the capacity and resources of government alone. There is a major role to be played by Startups and private investment to bring in additional human capital, financing, entrepreneurial skills, speed of delivery, technological innovation, along with the dynamic of the global Startup ecosystem.

Open Data stimulates innovation and Smart Buses

Startups bring a different mindset into GovTech, with their use of API's (standardised data transfer), Open Data and capacity to combine mashup multiple data sources they find previously hidden monetisation propositions.

Transport for London (TfL) is an example of what happens when public data is open, now with 11,000 registered developers, 600 travel apps and millions of daily API calls.

Citymapper grew up using TfL API transport data and has raised c$50m investment. Citymapper's journey has become circular, it has been testing out its own Green Smartbus on a central London route in collaboration with TfL. Maybe we have seen the birth of a data driven, on demand, adaptive bus service or digital transformation at a bus stop near you.

Private Sector Investment - What has the PE VC sector been investing in.

Almost unnoticed $1bn has been invested in GovTech with $75m in the UK. Large investments have been made, Accela c$235m developing Government as a platform, Nextdoor (c$210m) a private social media network. VC PE investors are specialising in the field GovTech Fund and Ekistic Ventures in the USA with a UK based fund Public.io now running a GovStart incubator programme.

The rise of VC PE and with Purpose Investors

A $40m investment into Change.org a social change platform indicates an appetite to invest into GovTech models by socially inspired investors such as Omidyar Network and Knight Foundation. This is an accelerating trend with Texas Pacific Group's "The Rise Fund" with Bono and Richard Branson as investors. In the UK Zinc VC is looking "to build commercially successful business to solve chronic social problems in the developed world" led by a very experienced investor team Saul Klein, Paul Kirby and Ella Goldner.

In FinTech Leapfrog Investments has invested in Insurance companies in Africa and Asia, an example is AllLife who has developed whole life cover Insurance for HIV positive and diabetic individuals in South Africa, it is now bringing it diabetics insurance model to the UK.

These investors look for the "double bottom line" Social Impact with Profit, bringing scaling size investment rounds and management expertise. : education, energy, food and agriculture, financial services,

M&A activity could become a hotspot.

At least 20 trade acquisitions have occurred, in the USA Maximus acquired Ascend and Acentia, Accenture acquiring Agilex, GovDelivery merged with Granicus, and Accela has been a leading consolidator acquiring companies to building up its portfolio. In the UK Streetlife was acquired by NextDoor. M&A activity could become a significant force in GovTech as existing suppliers many being large system integrators need to acquire new technology and business models.

So could GovTech become as large as FinTech?

Around $90bn has been invested in FinTech since 2010 (William Garrity Associates) in comparison $1bn GovTech investment is small, however we are at the very beginning of the investment cycle in GovTech. GovTech is now entering a new phase; Government and Civil society digital transformation models have been developed and proven both Government and civil society entities are poised to embrace Startup ecosystems and use PE funding capacity, dedicated CivTech innovation spaces such as the "The Rain Cloud" in Westminster London have opened.

Rocket Science an example of GovTech at Work

Elon Musk's SpaceX is an example of how Startup thinking can revolutionise a Government Institution. It would have been unthinkable 20 years ago to allow a Startup to use Cape Canaveral to launch the most sensitive of the US Airforce's satellites. Elon Musk went back to first (Startup) principles, what was the problem, what are the physics involved and asked questions - "Why throw away the multimillion dollar first stage booster". So while using very much the same infrastructure and people as NASA did, Space X, build, launch, recover and maintain Rockets at a much reduced cost.

Yes, GovTech investment and innovation could become as large as FinTech and this rocket is about to take off.

Ian Dowson, Co-Founder GovTech Research and GovTech Meetup London
Ian.dowson@govtechresearch.com, @govtechresearch

The Future Of Payments:

Sending Money Will Be As Easy As Emailing

Everyone today realises that the world is moving to a digital reality. Leading world digital agencies forecast that by 2020 the world's main channels of communication will be digital. We might expect that the same trend should be following in the payments infrastructure – something that would prompt a whole raft of disruptive changes in the market

Pavel KRAVCHENKO
cryptography, founder of Distributed Lab

Let's imagine that in the relatively near future - let's say 20-30 years from now - all financial processes would be automated and the global payments infrastructure would become entirely digitised. This means accounts could be managed, using digital signatures and that only the owner of the private key could carry out transactions.

Digital gaps

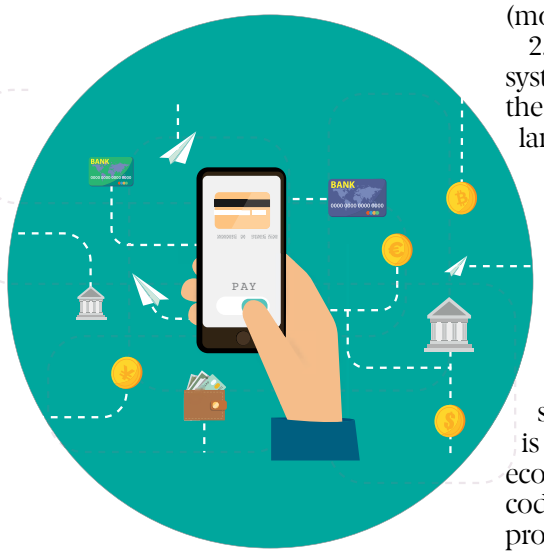
What does the payments infrastructure look like today? Today you have a wide choice of different communications methods to send a message to a friend in the USA or New Zealand – such as email, WhatsApp or Facebook - and your friend will get the message instantaneously. The contemporary payments infrastructure still lags far behind developments in the communications channels sphere. In this sector, there are a large number of rudiments and restrictions. You can not transfer money in just seconds from one part of the world to another, in a way that your intended recipient will get the money immediately. I ought to mention here that we are not taking into consideration services like PayPal, which offers the full package of services and benefits to those users who are regular clients. This business model very much look like a trusted bank model. Instead, we are analysing the future of global payment systems, that have many independent trust points.

Overall, payment systems are not efficient. There is a huge number of them and their integration requires a lot of resources. Each transaction can accrue commission payments (which are particularly high for international transfers) – and even so, the funds can still take several days to move from the sender to the recipient. Users have no clear idea how long the transfer may take, or how much commission will be charged – nor when the transaction might pass through the compliance processes. Payments can get lost during transactions between the parties. The level of fraud of internet payments is significantly high.

> We have grown so accustomed to the 'limited payment reality' that we can not even easily imagine how things could be different, or easier, quicker, or more efficient…

Limited reality

Let's try to figure out what makes it so complicated to pay online today? There are a number of explanations for this, but the key are interlinked with regulations (relatively minor), and outdated payments infrastructure (relatively major). I would offer to consider that problems in details. The main and most obvious problem is poor integration between various payment systems themselves. Globally monopolised payment infrastructure supported by the accustomed legal frameworks also play significant roles in this. One example is that many businesses prefer to accept only international payment cards as a means of payment – such as Visa, or MasterCard. Although there are other retailers, who only accept local payment cards. Vending machines might be restricted to accepting only low-denomination banknotes and coins. Minimum values for cashless transactions might be



charged a higher commission fee. The whole situation results in lost time and money for users. And here we are only discussing the payment infrastructure, not even touching on the topic of fund markets or similar.

One more problem is that the market for payments processing is extensively monopolised by Visa, MasterCard, Alipay, PayPal, Swift, and several others. Monopolies along with closed APIs act to prevent direct collaboration and integration processes between incumbents and users, aiming to preserve their very special status.

Regulators fail to receive real-time market information. The advantages of advanced systems with closed proprietary infrastructure nevertheless inhibit large-scale innovation. You can create a superb mobile app – but it can not be used by many financial corporations at one and the same time.

What is interesting is that we have grown so accustomed to this 'limited payment reality' that we can not even easily imagine how things could be different, or easier, quicker, or more efficient. Yet even so, a new dawn is coming. Can you remember the last time you wrote a letter with a pen? Although it seems that the entire world has smartphones now, it was only 5-7 years ago that they first entered widespread use.

The payments infrastructure of the future

For the digital future of financial markets described to dawn, we need to proceed by using the following important principles.

1. All assets need to be saved in a uniform digital format (money, securities, etc.).
2. All asset management systems need to interact using the same protocols (e.g. as a language of communication).
3. Asset management systems need to be able to interact with each other on a principle of mutual trust.

To turn it into a reality, it will be necessary to agree on ways to reconcile independent accounting systems. What is important is the openness of the ecosystems – component code and basic modules, and protocols. Standards must correspond to Open Source principles, not require users to pay license fees, and all rules should be described in detail for all market participants.

This will drastically affect the role of states and regulators. It will change to that of 'founders of the game rules' and 'controllers', instead of 'central resource manager', as now. The role of banks will be in the KYC process, risk management, and the provision of infrastructure. The requirements of society will also undergo fundamental change – sending money will be as easy as emailing or sending a message in a Facebook chat, with the whole thing taking place virtually, with a single click, and in just seconds.

If to follow this scenario, we'll see a whole raft of positive transformations. Competition will appear on the markets. User software will be easily integrated with any accounting system. Security will rise, and asset management will be carried out using cryptographic keys. Online experience for users will become simpler and cheaper. A wide range of ways of making payments will be available, and at any specific moment users can choose

Startups to change the world

In partnership with DIA Amsterdam

Jamie
HALE
CEO & Co-Founder at Ladder

● There is a $16 trillion coverage gap in the U.S. between what people should and do have in place. This is an unnecessary situation for those people, their families, and their communities. Ladder has rebuilt life insurance to be instant, simple, and smart.

● People have come to expect digital, on-demand options for most things in life: you no longer have to call a travel agent or go inside a bank. It should be no different for life insurance; however, the reality is the traditional life insurance process is antiquated and burdensome, requiring in-person meetings with agents, physical paperwork, and long wait times. We at Ladder have streamlined this process, removing the hurdles and complexities.

● **Ladder has re-engineered life insurance with a new technology and consumer focused design.** We offer coverage up to $8 million with no fees, all because we want people to be able to get whatever they need whenever they want. We have taken a holistic approach. We haven't just slapped a front-end marketing engine on top of the existing process. Our integrated overhaul is much better for the user, and it's longer lasting. Ladder is refreshing and redeeming an important financial product, turning the life insurance industry right side up and back to where it's supposed to be.

● Ladder is disrupting the life insurance process with its direct-to-consumer process to receive instant coverage.

● Everyone in this industry should be relentlessly focused on providing the best possible experience for people to get the coverage they need. Insurance was first created centuries ago as a way for neighbors and communities to have each others' backs. For a small contribution, each individual could make sure the people they care about would be covered, if the unthinkable happened. Ladder is ensuring this service is easily accessible for everyone.

1

Jeroen
MORRENHOF
CEO FRISS I fraud, risk & compliance

● Insurance fraud is a challenging problem and its economic effects are significant: expected losses can be up to 10% of operational income. This affects businesses' financial stability and profitability. But most importantly it is the society that suffers. Payments of fraudulent claims have a substantial negative effect on the losses of insurers and therefore, on insurance premiums. As a result, money flows to the wrong people and combined ratios are put under pressure. So why should customers bear the risk caused by fraud? **FRISS strives for healthy insurance portfolios and supports honest insurance.**

● Insurers from around the globe rate the fraud priority level as a 7 out of 10 on average. The biggest fraud challenges for insurers are related to data: issues with data protection and privacy; inadequate access to external data sources, and problems with internal data quality.

Our platform connects over a hundred data sources in order to provide better risk assessment to insurers.

● Today, a lot of potential insurance fraud can be detected automatically, based on the insurance history or relationships of a customer. Additionally, insurance employees can be trained to spot potential fraud. If insurers start working together closely and share their data on both national and international levels, it would make the industry stronger against fraud. FRISS is there to help insurers in reaching these goals.

● A lot of (large) insurance companies are working on digitisation processes and core system replacements these days. Although this puts pressure on IT resources, do not wait with implementing a fraud detection solution. With relatively small efforts a system can go live within a short timeframe and deliver results: fraudulent claims that do not need to be paid out, less high risks that enter the portfolio and of course compliant with rules and regulations.

2

Chris
KAYE
co-founder and CEO of Sherpa

● It's no secret that most consumers have a less than positive view of the cost and experience of buying insurance, and they doubt that their insurer will come through for them when they make a claim. We are trying to fix that. We came up with is a very different model which cuts out a lot of the existing players across the industry and delivers simpler, cheaper and more tailored solutions to consumers.
We want to move away from the concept of separate products and towards a more unified approach of assessing each consumer's individual risks, and providing them with a single account that protects the things most important to them. It means providing unbiased guidance, creating a single underwriting journey, moving from commissions to a subscription fee, and (hopefully) resulting in a reduced overall cost.

● Part of the changes we want to make to the industry will come through new technology improving the user experience and giving the consumer control over their own data. But some will also come through a new business model with less layers, and a single underwriting process leading to a single insurance account.

● We are disrupting the industry in three ways. First, we are aiming to pass consumers' risks as seamlessly as possible through to Gen Re, cutting out a number of layers in the value chain. Second, we want to create a single underwriting journey across all of a consumer's risks, rather than having multiple journeys by product. And thirdly, we want to move away from commissions and towards a subscription model, which we think better aligns us with the interests of our customers.

● Insurance is one of the biggest fixed spend of the average consumer. And often it doesn't result getting the cover they need. We are not yet live, but our hope is that we can assist consumers to get the proper cover they need without it costing them the world.

3

Tom
VANDENDOOREN
Chief Business Development Officer SENTIANCE

● We apply data science to turn sensor data from smartphones and connected devices into rich behavioral and contextual insights: understanding and predicting how people go through their everyday life by mining and analysing raw sensor data. Our SaaS platform enables companies to enrich their first-party customer data with real-life behavioral data so they can deliver context-aware and highly personalised experiences. Our context intelligence platform supports solutions for Lifestyle Based Insurance, Contextual Commerce and Marketing, Smart Mobility, Connected Health, Smart Home and Smart City.

● Ultimately, it's all about customer experience and how companies can excel at preempting and addressing highly individual needs in the moments that matter most. At Sentiance we have coined this the 'Internet of You' by enabling smart connected devices and applications to learn from your behavioral patterns and interpret context and intent, so they can adjust to your specific needs in real-time.

● **We use cutting edge technology such as sensor fusion and machine learning to enable new ways to engage and deliver value to users and customers.** By shifting the paradigm to behavioral and context-led propositions the core premise of many industries is being shifted as well: from marketing to engagement, from protection to prevention, from support to coaching, from service to assistance.

● Our core purpose is to become the context engine for the Internet of You leveraging our core expertise in behavioral analytics based on observed data. We look to inspire our customers with use cases from multiple different industries and geographies, and assist them in building out deeper and more valuable relations with their end-customers. It's very early days, but our contribution to enabling the Internet of You will hopefully be seen as something highly positive and rewarding, to the common benefit.

4

Startups to change the world

In partnership with Disrupts Magazine

Pavel
KRAVCHENKO
cryptography, founder of Distributed Lab

Distributed Lab is a crypto and decentralised technology expertise center.
Our main activities are creation of digital payment infrastructures and application of blockchain solutions to business. We solve the problem of the global payment infrastructure accessibility and security, and create turnkey solutions which include integration into legacy frameworks, business architecture creation and user experience.

The world is getting digitised and the payment processing infrastructure has to move ahead too, towards being faster, easier, smarter, cheaper and available for all the customer categories. Currently it is heavy-footed, slow, closed, extremely expensive and monopolised. Scaling our solutions across the world could help New Gen payment services to get mass use.

The first and the biggest challenge for the blockchain industry is inflated expectations around the technology itself. Being influenced by overly positive newstream, blockchain is expected to be a 'magic pill' and to solve all the problems with transactions' security and speed, data transparency, KYC and many more... However, it is impossible to solve those issues without crucial changes in existing global accounting systems and business processes.
We have put a lot of effort so far into explaining what blockchain is and what it is capable of doing.

We believe the future of payments to be digital, instantaneous and free, with transactions being confidential (however subject to AML/KYC), with the source of funds origin being proven and the accounts controlled solely by their owners. It is not easy to create such a future considering the money origin challenges and problems in the global payment infrastructure as of today, but this future will definitely come.

5

Joanne
DEWAR
Chief Operating Officer at Global Processing Services (GPS)

Creating C-Level Opportunities for Women in Fintech

Fintech is seen as being both innovative and disruptive. However, could more be done in this revolutionary space to encourage females who have taken a career break from senior roles to come back to work?

I took a career break to be a full-time mum. This is a hard decision many women in senior level positions make. Their professional talents are 'lost' in family life and their identities become more about their position at home. Returning to work can become a challenge and reclaiming those big roles can be even more difficult.

Some financial institutions, such as JP Morgan, have launched 'Return to Work' programmes, but growing fintech companies could provide more opportunities by extending their progressive ways of thinking and doing things outside the norm.

Research in a 2015 report entitled 'Power Women in FinTech Index: Bridging the Gender Gap' suggested that organisations founded by women or that champion leadership roles for women in fintech are more innovative and return better results.

With that in mind, I am a strong advocate for re-engaging this 'lost' pool of talent and creating the right opportunities to enable women – and men – to resume their careers.

My employer allowed me to return gradually, progressively increasing my time and responsibilities in the workplace, as the responsibilities of home life decreased and my confidence returned.

However, there are many barriers to address in returning to work at this level and companies need to look at what they can do to create opportunities to attract female C-level talent. There are real opportunities for financial services and technology companies to differentiate themselves and become more successful by taking advantage of this pool of lost talent. Entrepreneurs are ideas people and have the power to open more doors. Let's get our thinking caps on!

6

Mihai
IVASCU
CEO and Founder of Moneymailme

Ideas to change the world – social money transfer

The world of finance has changed almost beyond recognition in recent decades and today's millennials are driving forward brand and product innovation as companies try to adapt to 18-35 year olds' demands. Millennials want collaborative technology and they expect it fit in to their interconnected lifestyles. With the world becoming smaller and smaller, technology solutions must be efficient, easy to use and allow people to communicate internationally instantaneously. Consumers now want, and more importantly need, to send money globally with the knowledge that their recipient will receive it immediately. In the world of FinTech, this idea of collaboration is really at the heart of it all. We believe in the power of an app to let consumers send and receive cash while chatting or video calling. Ease, speed and collaboration are key, whether sending money to friends abroad, paying back family members, donating to a charity helping to save rhinos from poachers or finding a solution to build a solar powered school in Zimbabwe.

This point around charity donations is very important to millennials, half of whom (48%) believe that physical money will be obsolete within 20 years and 62% of whom feel frustrated if they are forced to make purchases with cash. Our own research, which surveyed 1,000 18-25 year olds around the UK, highlighted that it is important there is transparency about where charitable donations, with over a third (35%) saying that they would use a mobile app to make donations as long as they could clearly see where the money was going. Nearly a quarter (24%) would do so as long as there was no charge.

So whether charity donations or micro transfers to family and friends, we believe social money transfer is the future and will change the way we interact with money and serve the millennial market.

7

Simon
GILBERT
Managing Director and Founder at Elmore Insurance Brokers Limited

Don't leave the Homeless behind

We are speeding towards a cashless society. Credit & Debit cards now swipe their way through the simplest of transactions. Soon even our wallets will become exempt as contactless chips are embedded into our devices, wearables and possibly in the not too far future even into us. While this provides many benefits of convenience, a future cashless society leaves a dilemma for the unbanked homeless.

There are over 250,000 homeless people in the UK and over 100 million world-wide, but how will people show their spontaneous generosity in a future cashless society?

The Elmore Fintech Insurance Team want to change the world by bringing a robust and low cost contactless payment infrastructure to the homeless.

A perfect partnership between FinTech and homeless charities.

Homeless people could be registered with a wearable card reader which could be biometrically authenticated to the person, at the same time a pre-paid account with the charity could be opened in the person's name.

Quite simply any donation the person receives, 1/3 go to the charity to further their cause and 2/3 would be accessible in credit for the person to receive meals, clothes, blankets, and other services required in times of need.

Anyone could choose to donate by simply tapping the card reader which could be fixed at £5/£10 per transaction. Donors could be rewarded by governments (using a clear audit trail) for their donations by a reduction in their tax bills.

Contactless payments could revolutionise people's instinctive kindness, in a considerate and convenient way, ensuring donations make a real change when they are most needed.

8

"AI QUEEN"

Joanne Smith

CEO, Recordsure

● Is it difficult for a woman to build a career in Tech?

- Tech is a male dominated industry and this is means that women don't often see themselves succeeding in a tech career. On one hand, getting women into tech is about making sure they have opportunities to learn the key skills. The number of initiatives which are helping get women and girls into coding are a great example. But on the other hand, companies need to get more serious about workplace diversity today, otherwise the next generation of girls won't be able to see role models among the ranks of the big tech players and might be discouraged, even if they have gained the skills they need.

● What are the key differences between senior roles in a corporate as opposed to running a tech business?

- Having worked in corporates, I know all too well how decision making can be political and slow. This especially true for women as we were never taught the rules of engagement! Running a tech business is fast-paced. Our team can see decisions become action in almost real time. Of course, one of the pitfalls of success in a tech business is getting larger. The growing pains of the company are acutely felt by the founder, whose once scrappy team is suddenly much larger and less nimble.

● How did you get the idea of your startup - why AI?

- Part of being an entrepreneur is about being brave enough to believe you can solve a stubborn problem. I think you need to be especially brave to try and solve a problem that you are an example of. I had been working with my team in compliance consulting for decades. We knew the limitations of how our advice was being applied by financial institutions. It was clear that a scalable technology solution could fix a lot of what banks were struggling with. In short, instead of trying to use the same limited tools to solve expanding problems, we starting thinking about how we could expand the tools. AI is a brilliant new frontier in this regard. It help makes the human input, which remains so critical, have a much greater impact.

● You gathered an amazing team - data scientists and linguists from Cambridge as well as lead engineers of Apple's 'Siri' to develop Recordsure. How did you motivate them to join your startup?

- Tech companies often get evaluated on the quality of their "talent." We certainly fortunate to have a highly talented team at Recordsure. During our hiring phase, we found that Recordsure appeal to some really brilliant people for two reasons. First, they were excited to be developing a first-of-its-kind product that is difficult to create. This is real innovation. Second, individuals were excited to work on a project with people with very different talents and background. In bringing engineers, scientists, and linguists together, you ended up with a much more dynamic workplace. I think companies should embrace diversity in talent-- it helps attract the best and brightest people.

● What is the main problem your business is solving?

- Recordsure makes it easier for large banks and financial institutions to ensure that their employees are conducting themselves to the highest standards and looking out for the interests of customers or clients. Our technology helps companies record and analyse conversations with customers to make sure that the right information is being shared in the right ways so that both the customer and the bank have better outcomes.

● What are the major challenges for your business?

- Financial institutions are large and complex organisations. Anytime you want to institute a new technology or a new type of process you will encounter challenges. The organisations we work with very quickly understand the value of our solution, but it can take a bit longer to find the best way to implement it!

● Do you see applications of your business activities in the field of financial inclusion? (It's totally fine if you don't!)

- Although we are currently focusing on a rollout with financial institutions, we see lots of potential applications wherever a sensitive conversation is happening between someone providing advice and a client. For example, the ability to better monitor conversations between doctors and patients could offer health services an ability to fine-tune their healthcare.

● What is the major social impact your business has delivered so far as you see it?

- We believe that our platform will improve the quality of service that banks are able to provide their customers. More transparency and better compliance monitoring should help protect the interests of the public in many ways.

● Your piece of advice to women in tech?

- Never doubt that you could be the first person to have an excellent idea.

Recordsure was founded in 2011 by Joanne Smith. The concept for Recordsure emerged from Joanne's 20-year career in financial services and her subsequent role as CEO of TCC, the UK's largest leading provider of compliance solutions. Prior to founding TCC, Joanne held senior roles at leading financial services organisations including HBOS and KPMG. She also worked as a regulator at the FSA. She holds an MBA from Ecole Nationale des Ponts et Chausées in Paris. Named Women in Compliance Awards' first Inspirational Woman of the Year in 2014, Joanne is also a Natwest Everywoman Award nominee. This award recognises female tech entrepreneurs developing real-world solutions to help build a smarter planet.

In 2012, seeing a gap in the face-to-face advisory market, Joanne realised that technology could help solve some of the complex compliance issues affecting financial institutions, as well as the potential for future mis-selling (which has cost UK banks over £53bn in the last 15 years) and poor advice issues for customers. It was then that Joanne committed substantial finances to research and development for a technology product that could be supported by the existing expertise and industry knowledge of TCC. She employed a raft of data scientists and linguists from Cambridge as well as the lead engineers of Apple's 'Siri' to develop Recordsure and now has the most advanced AI conversation analytics on the market. She received £14m in funding from the Business Growth Fund.

Diversity and the future of startups

by Toby KRESS

The UK startup scene has seen a surge in popularity in recent years, with record-breaking numbers of new businesses founded in 2014[1,] 2015[2] and 2016[3]. But while the bigger picture focusses on an industry going from strength to strength, a closer look tells a more nuanced story and highlight one major failing: UK startups are severely lacking in diversity.

In fact, while the UK in general is more diverse than any other major startup ecosystem[7] that advantage hasn't translated into a similarly diverse startup community. Those who work in the startup economy know it is disproportionately white, male and relatively wealthy.

To understand this let's start by looking at the importance of money in starting a business. Research published by Crowdfinders and IW Capital[5] found that over 50% of company founders said that money from family members had been integral in starting their business and 45% had used finances from friends.

In addition to this, the research looked at the most popular routes to funding for entrepreneurs in Britain and reported that:

35%
used personal savings

28%
used banks and institutions

15%
used friends and families

This is pointing out the obvious, I know, but it's important to note the fact that many aspiring entrepreneurs don't have personal savings, would not be able to borrow money from banks and institutions and are not able to ask friends and families for financial help.

At London Met University we run entrepreneurship programmes for student and graduate from an incredibly diverse set of backgrounds. Most of them don't have savings or access to family money to get started. This means they have to work full time while trying to get their idea of the ground, which often proves impossible.

The effect of this is the startup industry is losing out on a huge untapped pool talent and creativity.

The good news is that the cost of starting a business has dropping through the floor in recent years so it doesn't take that much to get started. The winners of our Big Idea Challenge competition share in a prize pool worth £30,000 and we have seen that a small amount of cash can go a long way in the early testing phase - with previous winners using their prize money and the support of mentors to start businesses that are thriving years later.

As well as the wealth and class issue, business owner Suzanne Noble points out that "Ageism and sexism are rife"[6] in the UK startup scene.

This often-repeated opinion is rooted in fact, with women making up only a third of the UK's entrepreneurs[7] and only 17% of US startups have a female founder[11]. This may be due in part to traditional gender roles, or the fact that gender has been proven to affect funding, with women being less likely to get VC or angel funding and more likely to be self-funded4. In First Round's State of Startups 2016 report8, 700 surveyed startups were questioned on the male to female ratio of their teams. Their answers were telling with 61% of startups being mostly or all male and only 8% mostly or all female.

What's even more telling is that, in this report, "diversity" appears to refer only to gender - and not to race. While the male to female ratio of boards and teams was evaluated, race wasn't. At all. According to a survey undertaken by Tech London Advocates when 200 tech leaders were questioned, only 9.4% believed multiculturalism drove their enterprise[9]. This is in stark contrast to comments made by Lawrence Wintermeyer, CEO of UK's FinTech membership association Innovate Finance, who said that "Diversity... brings new ideas for services and different solutions to problems in a world of changing markets and customer demands. It also brings a range of skills, experience and cultural understanding to inform companies. It is a reality that we must all embrace. Inclusion is the solution for a better future for everyone."[10]

So, what does this mean for the future of startups? With an increased focus on representation, there is a drive towards creating diversity in the startup industry. And the fact is that companies not only have a moral and ethical reason to recruit diversely, but many business reasons, too.

London Met Uni's Big Ideas Challenge is one of several initiatives created to even out the playing field, so to speak, and push the industry towards a truly representative workforce. Initially started to discover and support entrepreneurial talent amongst London Met's student body, this year the university was joined by 17 competing colleges from across the capital, whose students also reflect the broad diversity of the city. For many of the young people taking part it was their first exposure to the world of entrepreneurship and for some the start of a long and rewarding journey.

Throughout the competition, the students gain core skills and knowledge with the help of some incredible mentors from corporates such as NatWest and Microsoft, non-profits including the Prince's Trust and founders of successful startups. On "Bootcamp Day" it's incredible to see them transform from nervous wrecks when they first meet their mentor into empowered budding entrepreneurs by the time they pitch to a live audience at the end of the day.

Building confidence like this is a crucial part of opening the door to entrepreneurship to young people from all backgrounds. No matter how smart, imaginative and driven students are it takes someone to recognise that and give them the confidence and support to set their aspirations high.

Excitingly, this year's winners of the Big Idea Challenge were presented with their awards by The Duke of York at St. James's Palace – both validating their hard work and inspiring them to take their ideas on.

With their new found confidence, network, support and a small about of money we hope many of these young people will go on to start successful companies. And at the same time make the startup world a more diverse, interesting and successful sector.

[1,2] Britain hits record number of startups as more aspiring entrepreneurs take the plunge, The Telegraph
[3] Record 80 new companies being born an hour in 2016, The Telegraph
[4] Opinion: London's 'amoral' tech elite is driving inequality, wired.co.uk
[5] Is equity crowdfunding truly democratic?, crowdfinders.com
[6] What 2015 taught me about the London tech scene, Tech Crunch
[7] Diversity vs. class in UK's startup scene, IDG Connect
[8] State of Startups 2016, firstround.com 9
[9] Tech still trails: Half of London's tech sector believe bias against women exists, startups.co.uk
[10] UK MORE DIVERSE THAN OTHER MAJOR START-UP ECOSYSTEMS, INCLUDING THE US, SILICON VALLEY, NYC AND TEL AVIV, wayra.co.uk
[11] Opinion: London's 'amoral' tech elite is driving inequality, wired.co.uk

SPONSORED BY THE MONTCALM ROYAL LONDON HOUSE

Luxury treats for Men and Fathers this June

Emily
MANSON

June sees a lot of Father's Day fuss but we don't think a day is enough. This column is all about little luxuries whatever the time of year, but in keeping with the spirit of the month, we've dug out those special things that really would make any man or dad's – day, week, month or year. So whether you just want to spoil yourself or treat a man in your life, these gorgeous luxuries are sure to please.

There's something undeniably indulgent about a hand-crafted leather briefcase. **The J Style Two Pocket Briefcase from Picketts & Co** is handmade in England by British craftsmen inbeautiful quality naturally tanned bridle leather. It comes with a traditional polished solid brass lock in black, brown or tan options and is a classic that's set to endure and give pleasure for years. (from £675).

Even in this IT-age, there's still nothing more decadent than a fountain pen. The new **Lamy Dialog 3 Pen** with its 14k gold nib and special cap-less twist design, gives this classic pen a modern yet highly practical edge – the newest gadget pen around – and it's available in palladium and black. (£229.50).

As gadgets go, this must be up there as one of the best for small gardens. The robotic lawnmower, Robomow RX has been designed specifically for smaller London gardens and mows automatically at regular intervals, leaving you free to enjoy the post-mow cold beer a little sooner! (£500).

For a little grooming luxury, **Legends of London** offers the finest authentic products with modern flair, from their hair gel and pomade designed by traditional barbers, to their 100% natural Alum matches which come in a handy matchbook size. These scooped Best Beauty Product 2017 and are great for soothing razor burn and irritated skin on the run. (from £6).

It's not often you'd put men & cushions in the same sentence, but award-winning and renowned London designer Andrew Martin has really hit the spot with these **retro Beatles tapestry cushions** in red or taupe. Handmade in the UK, they picture the iconic Fab Four during their Sergeant Pepper era – and look great as a contrasting pair (£49 each).

Foodie treats come no finer than the award-winning **'Man Box' from London's Ross & Ross Foods.** Containing a brilliant selection of must-have-man-goodies, it includes beer, chutney, salami and crackling (from £21 to £40). They also offer home cure kits for aspiring chefs as opposed to dedicated gourmandes.

Gold Icons Godiva chocs

Beatles Taupe Cushion

And finally, who doesn't love a box of chocolates to spoil someone whether it's Father's Day or not! These new **Gold Icons from Godiva** are deliciously moreish with fabulous flavours and bound to disappear quickly, father or not! 6-piece/18-piece gift boxes are available. (£10/£25).

The Legends London Pomade

Where to find these little luxuries ...

- thelegendslondon.com
- andrewmartin.co.uk
- penheaven.co.uk
- www.pickett.co.uk
- robomow.com/en-GB
- rossandrossfood.co.uk

The J Style Two Pocket Briefcase from Picketts & Co

If you want to be featured in the lifestyle section, contact
katia@fintnews.com

June 15

The Economist Events' Impact Investing Summit@ London

Join editors of The Economist and more than 200 leading financiers, institutional investors, policymakers, academics, impact investors and philanthropies, to discuss: What are the next steps in growing the impact investing movement? Is the recent commitment of mainstream finance to impact investing more than skin deep? Is it possible to build 'impact' into the very fabric of traditional investment firms? You can benefit from a **20% discount** on the current rate of £895 with **code FINTECH/DC.**
impact-investingeurope.economist.com

June 18-20

Global Expansion Summit @Intercontinental 02, London @ Intercontinental 02, London

Advance your international and cross-border business strategy at the Global Expansion Summit in London from 18 to 20 June 2017. The Global Expansion Summit brings together 400+ C-Suite and 50+ Heads of International Expansion from 700+ companies and 62 countries to help advance international & cross border business strategy. Key 2017 themes include Innovation, Fintech, Global Talent & Mobility, Global Supply Chains, Logistics, Outsourcing, FDI, Market Profiles, Risk Management to learn from each other and advance international & cross border business strategy. Use discount code GXP30 at checkout for 30% off. For more information, visit the Global Expansion Summit website.
www.gxpsummit.com

June 26-28

Money 20/20 Europe @ Copenhagen

A world-class experience for European innovators across industries and company types, #M2020EU is more than just an event. It's a catalyst for the growth and development of the payments and financial services ecosystem.
Use code FINTIM2017 for an extra €200 off
www.money2020europe.com

July 7-14

Fintech Week 2017 @ London

Expect 600-1,000 conference delegates per day from over 50 countries and 3,000 – 5,000 participants in events throughout the week.
The limited offer '2-for-1 Full Conf Pass' is still valid.
www.fintechweek.com

December 6-7 London

Fintech Connect Live

Combining the hustle and bustle of an exhibition featuring over 3000 visitors, and 200 exhibitors and partners from over 50 countries, FinTech Connect Live is the UK's largest fintech event. Playing host to 4 strategic conference sessions with inspirational case studies from around the world, a technology buyers theatre with 50 product demos, 12 educational workshops tackling practical fast growth challenges, and two full days of dedicated mentoring clinics for start up leaders, all brought to you from over 300 of the industries finest speakers, FinTech Connect Live is the 'must have ticket' for stakeholders from across the full fintech eco-system.

FinTech Connect Live provides a platform for all those attending to collaborate, differentiate, form connections, source solution, conduct and generate business with new, existing and upcoming fintech players in the market.

Get involved and find out more by visiting www.fintechconnectlive.com

fintechconnectlive.com

SHOWCASE YOUR COMPANY TO THE WORLD

FINTECH WEEK LONDON 2017

NEW FOR 2017: 2 FINTECH EXHIBITIONS & FINTECH JOB FAIR

HACKATHON WEEKEND	DAY 1	DAY 2	DAY 3	DAY 4	DAY 5
07	08	09	10	11	FIRST FLOOR 12
	SATURDAY	SUNDAY	MONDAY	TUESDAY	WEDNESDAY
	Hackathon	Hackathon	Money & Payments + Showcase	Capital Markets + Showcase	London Fintech Exhibition
			Conference	Conference	Exhibition
			8am-5:00pm	8:00am-5pm	9:30am-4pm
FRIDAY					
Hackathon			Opening Drinks	Fintech Tuesday	
hackathon kick-off			drinks reception	networking drinks	
6:30pm-9:30pm			5pm-8:30pm	6pm-9:30pm	

FIRST FLOOR 12	FIRST FLOOR 13	FIRST FLOOR 14
WEDNESDAY	THURSDAY	FRIDAY
International Fintech Exhibition	Blockchain & Cyber Security + Showcase	Fintech Job Fair
Exhibition	Conference	Job fair
9:30am-4pm	8am-5pm	9:30am-4:30pm
Evening Drinks	Silicon Roundabout	
drinks reception	networking drinks	
4pm-8:30pm	5pm-9:30pm	

14
FRIDAY
Partner Workshop Day
Multi-location workshops
9:00am-4:00pm
FTW Closing Drinks
drinks reception
5:30pm-9:30pm

BACK FOR A 4TH YEAR

JULY 7-14

EXHIBITION/SPONSORSHIPS AVAILABLE

sponsor@fintechweek.com +44 (0) 7968 910744

www.fintechweek.com

FINTECH WORLDWIDE LTD. Linklaters Pinsent Masons