January 2016

The Fintech Times

TheFintechtimes.com

An independent business newspaper

Cybercrime is normal

(p. 3-9)

What is Fintech?
The Future.

FINANCE + TECHNOLOGY

Fintech is a new definition, but one expected to become normal. Fintech is the future of finance, of financial services, and indeed of money itself. For those already in the know, this is not news.
Fintech isn't a business sector; it's dozens of sectors. Everything from high street banks, investment companies, money transfer, fintech is re-engineering these sectors into their next generation. And there are new kinds of businesses emerging within fintech: crowdfunding, peer2peer lending platforms, crypto currencies, the Internet of Things, sectors that are digitally native; they didn't exist before the internet.
And cyber security, this month's cover story.

There's many ways to look at fintech. It's about new companies, and new technologies for old companies. It's about inventors and visionaries, and everyday people creating something new. It's about your bank, your phone, and your job. It's about you today. It's about the future.

And it's definitely about change. Big big change.

A fintech newspaper?

People like newspapers. They can be a three-minute read between tube stops, or a Sunday morning in bed. So what kind of newspaper is this?

There's so much happening in fintech, it's so interesting, and sometimes so complicated, and we think it needs its own monthly newspaper as an industry report. That's what The Fintech Times is.

Who for?

For company directors, entrepreneurs, and managers, business minded people. It's for everyone in finance, banking, and investment. Anyone in tech and anyone interested in startups. Because fintech is where the money is.

Format

Each month we will be exploring a new fintech sector, interviewing thought leaders and experts, digging deep into the ideas, people, and technology. Then taking that experience and presenting it in a format that you can read at your leisure. We plan to keep it intelligent, investigative, authentic, but not too serious; informative and useful, but not too technical. Enjoyable. Let us know when we get it right or wrong.

So...

Keep your copy, start subscribing, become a member, or partner. Watch the changes happen. Be involved if you choose. Fintech is new. And Fintech is the news. London, by the way, is the World leader in fintech, and long may we be so. Not that we don't welcome the competition.

Finally, to subscribe or become a member, to read and comment online, search thefintechtimes.com

Let us know what you think.

editor@thefintechtimes.com

The Fintech Times
Published by
Disrupts Media Limited
83-89 Mile End Road
London E1 4UJ
www.thefintechtimes.com

Editors:
Katia Lang
Bird Lovegod

editor@thefintechtimes.com
07535 670 581

COVER STORY: Cyber Security

Expert: Brian Lord OBE

Editor
BIRD LOVEGOD

Cyber Something: What's Happening?

Normalising the situation. Based on a meeting with Brian Lord OBE, MD of PGITL.

The first thing Brian draws to our attention is that technically Cybercrime doesn't really mean anything.

As a word, it's fresh from the late 1970's, cybermen, cyberspace, cybersexcitement. By definition it is 'something to do with computers, information technology, and virtual reality.' That narrows it down to everything in 2016.

This 'cyber opacity', in the context of crime, equates to a fog of understanding that makes it difficult to do anything meaningful.
"We, meaning businesses and organisations, need to treat 'cybercrime' as a normal risk."
One of the repeated points Brian makes is that cybercrime, (maybe we should call it something else) needs normalising. This means stripping away the mystique and techspeak and understanding it in a rational and 'real world' compatible way. The use of jargon, buzzwords, and media hype obfuscates and disguises what is actually a number of completely separate issues and risks.

Brian takes it back to basics.
"So let's treat 'cybercrime' as normal. It's just bad people doing bad stuff, the same bad stuff as has been done for thousands of years. Breaking and entering. Theft. Vandalism. Espionage. Blackmail. Ransoms. Crimes as old as civilisation. The only new thing is the vehicle, the means, by which these nefarious activities are actioned."
The game changers in cyber crimes are scale, speed, location, and traceability in relation to what the media casually calls attacks. A single bad operator can command an army of ten thousand computers against a company or organisation. Clearly the speed of events happen at the speed of digital transmission. A problem becomes an unmanageable cascade of bad news data in literally a second. Location of the attackers? Could be anywhere.

> *"Let's treat 'cybercrime' as normal. It's just bad people doing bad stuff, the same bad stuff as has been done for thousands of years."*

The challenges and complexities of information security make it especially important to use a normative approach in business. Even calling cybercrime by the more correct term of information security is helpful. Information is a thing, you know what information your company has, and where; what is important, and what is critical.

Let's call it information security from now on. Brian uses real world analogies; how supermarkets protect tins of beans differently to bottles of spirits.
Imagine your house. You close the doors. You lock them. You keep windows closed. But someone can still pick a lock or kick down a door. So you look at what is valuable in the house, and you keep it out of view. What is really valuable, you keep in a safe. Then you look at what is critically valuable or sensitive, and perhaps keep that in a security deposit box in a bank.

You do what is reasonable to keep thieves out. But you acknowledge that thieves might still get in. If they really want to, they will. So you take reasonable precaution, have a contingency plan, and maybe an insurance policy. "There's no point in having an intention of 'make sure we never get hacked'. That's not realistic.

It's not about trying to become an impregnable fortress. It's about being proportionate to the risk. Like any normal business risk."

Back to business: How to normalise information security procedures? It comes down to understanding the specifics: Specific threats, specific sectors associated with those threats, then threats and risks specific to your organisation, and the specific departments, the specific IT hardware, and the specific individuals using it. You really only need to know and care about risks that are relevant to your company.

This is so obvious in the real world it's normal thinking. And this is what we mean by normalisation of risk, threat, and response. Information has value. Some information has more value than other. Protect accordingly. Human error is always going to be the weakest point in the information protection process. Therefor the first and most important response is education, training, and understanding the realities of business in 2016. It's no big deal. It's just another normal day.

Brian Lord OBE

Prior to joining PGI, Brian was the Deputy Director of GCHQ for 21 years, wherein he was responsible for Classified Intelligence and Cyber Operations. During that period, Brian directed the growth and perpetual evolution of departmental capability against emerging threats. He planned and ran both defensive and active Cyber operations, applied through unparalleled experience of cyber threat, risks, opportunity, and effective mitigation strategies. He culminated his career at GCHQ as an eminent thought leader on the subject of cyber warfare and on the intent and motivations of cyber threat actors.
At the time of departure, Brian also had overall GCHQ Senior Civil Service responsibility for the development, capability building, and requirement setting for the active defense and offensive Cyber capability and chaired the relevant joint GCHQ-MoD Programme Board.
Additionally, Brian developed operational coherence across both foreign intelligence agencies for his areas of responsibility; his experience extends to both the design and participation in cross-government National Security exercises.
At PGI, Brian has designed and delivered the PGI Cyber approach to organisational transformation and skill development, whilst growing and maintaining relationships with government and industry professional bodies, as well as the relationship with Academia within the Cyber Academy. Brian currently personally oversees all capability delivery for foreign governmental clients. Brian is regularly enlisted by the BBC and other national media outlets as a specialist spokesman on Cyber matters.

COVER STORY
Cyber Security

CYBER HYGIENE

Sector Specific Threats

by BIRD LOVEGOD

Not intended as a complete 'how to' guide, but more a guide to a normative approach.

Threat:
Malicious attack / Blackmail / Ransom
Sectors:
Public sector, third sector, corporations, controversial sectors, charities, animal related including farming, meat production, sex / gender related.
Sony found themselves on the wrong end of what could genuinely be called an attack, in retaliation for a film parodying the North Korean leader. This was an attack, in so much as it was a deliberate and sustained act of malicious activity designed to inflict harm.
But that's at the top end of business and global politics, not really relevant to your dating website company, right?
Ashley Maddision was penetrated in an attack designed to collapse the company, either by the directors closing it according to the ransom, or through reputational damage from the exposure of the users on the public web. Coupled with this the exposure of AM's own rather underhand practices of creating female accounts in bulk in house to balance out the gender gap. The company technically survived, its reputation in tatters, CEO gone. Hmmmm.

Brian Lord told us of a charity recently fined quarter of a million pounds for their data breach. They operated an invaluable service to support women in their extra-ordinarily difficult decision making process regarding unenviable life choices about childbirth. Ahhhh.

Questions: Could we be severely provoking any individuals or groups? (This is not the same as doing anything wrong.) If the answer is yes, and they are likely to feel justified in attacking you, if you offend their morals, ethics, religion, or politics, you may want to think about this threat in a way a florist probably doesn't need to. The information you hold might not be valuable in the same way credit card details are, but may be excruciatingly sensitive.

Threat: Theft*: All information has some value. All. If someone else had it, how much would you care?
*Theft used to mean you no longer had something. Now it means you have it, and so does someone else.
Sectors: Most sectors, but some much more so than others. From law firms holding IP and contract information to anyone holding payment info, contact details, even email addresses. The more comprehensive the data, the more valuable. Email addresses alone are of small value, add a bank name and it becomes much more valuable, a home address, more, account numbers, even partial, more, and so on. The more specific the information, the more valuable. Client X is negotiating a merger with Y and will accept Z pence per share. Multimillion pound information in the right / wrong hands.

Questions: Imagine all your information was in paper form in filing cabinets. Which of those cabinets would you really not want photocopying and distributing to the public? Which contains your organisations information, and which your customers information? Which do you protect more? How are these filing cabinets labelled? Do you have one labelled "Extremely Valuable: Do Not Photocopy"? Is that the best label for it? Do you have a system admin account named "Sysadmin"? Is that the best name to call it? Think about whether you would leave a sign outside your house with an arrow saying "Spare Key under this Plantpot – once inside follow the arrows to the safe".
Risk analysis should be undertaken to understand what information you hold and the potential value it has, generically, and perhaps very specifically. You may find the process itself rather useful.

Threat: Data Manipulation
Sectors: All fintech + others
This may become much more of a problem than data theft. It may already be so.
In 2013 a large bank robbery involved digitally removing the withdrawal limit on pre paid debit cards and then cloning them. It resulted in a loss of over £20 million in cash. Cash! Taken from several thousand ATM machines in multiple countries in just a few hours. Changing information may be more valuable than 'stealing' it.
Questions: What information do you have that could be manipulated or changed within your system? Credit limits, for example. Or account balances? Do you have checks and measures to prevent this? Or a procedure to notify admin of sensitive changes? Response time?

Threat: Spearphishing
The targeting of specific individuals within an organisation at specific points in time, to achieve a single target aim. Either to elicit the individual to directly disclose some information, or carry out an act, such as making a false payment or to encourage the individual to open a folder or go to a website that will automatically download malware for other criminal purposes.
Example: a sales contract has just completed. Payment is due. The account manager receives an email from the customer thanking him for the excellent service, wonderful delivery of product, we'll be sure to use you next time, and one last point, could the balance of payment be made to a different account number. Have a great day.
Sectors: Many, including manufacturing, export, but especially non end to end digitised companies, as this type of fraud involves 'social engineering', or more accurately, individual to individual deception.
Questions: Does everyone in the company know this kind of fraud exists, and are aware of the variations of it? Are there procedures in place to double check account changes, specifically payment transfers, in a non digital way? Like a phone call?

Threat: Downloading / installing Malware: Could be anything, from ransom-ware that encrypts your computer to spyware that facilitates spearphishing.
Sectors: Everyone, including individuals.
Example: you all get an email. Redundancy notices for 2016. See attached list. What percentage of employees open it? You go to an event. You are given all sorts of goodies, including promotional USB sticks, perhaps from another visitor who you also give your business card to? And so on.
Questions: Is everyone in the company aware of these risks? Without being paranoid, are they being conscious and careful. If you don't know the person, probably better not to put it in your computer?..

COVER STORY
Cyber Security

The psychology of teenage hackers|

As with 'non cyber' crime, the perps range from Nation States to organised crime networks to teenage kids. Perhaps by understanding the mind-sets we can begin to understand the problem. A bit.

One of the 'problems' is that people do online what they wouldn't do in real life. Connected, we are detached from each other, our nuanced communications reduced to the digital equivalent of shouting abuse at fellow car drivers who swerve into our lane. Only it's more than that. Our digital presence can take on an identity all of it's own, a digital persona, and that persona can be more influential, more exciting, more alive, than the one IRL. (In Real Life)
Here's how Brian Lord from PGITL describes the situation.
Twenty years ago there were checks and balances growing up, parents tended to know roughly where the kids were and what they were doing, the school teachers knew the parents, as did the local police when they needed to, and peer groups were small, a dozen maybe. Life was goodish, and these societal checks and balances tended to stop young people being overly criminal.
Now, in 2016, most teenagers spend more time interacting online than offline. So where are the checks and balances now, and who are their peers?

Ones thing is for sure. The parents can't answer that. And nor can the teachers. And online, there are no local police. Nor is the peer group restricted by age, or location, it can number thousands, and many of them have an un-connected online and offline identities. And the places to meet are unlimited.

For one generation, this is worrying. For the other, this is normal. There's a gap, native and non-native digitals, and it's wide. The real world checks and balances, the police, teachers, society, these have had hundreds of years to develop and embed within society and have evolved hand in glove with society as it changed. The digital mutation that is the Internet has non of the old World legacy, and youngsters can spend most of their time in groups of other people who have normalised what technically is cyber crime. Maybe it starts with hacking a school friend's facebook page because they dissed them on Kik. It's like tagging a wall. No big deal. Being initiated into the world of cyber crime is very easy; the slope unperceivable when it starts. Talking through Xbox, playing COD, already they are in a world that excludes their parents, the authorities, the teachers, the police, everyone and everything non virtual. It's now normal to have dual identities, one online, one offline. Normal is relative to ones peers.

Would a fifteen year old walk into a bank and rob it, just to see if they could get onto the league tables of coolest bank hacks? And yet digitally, it's virtual act. Not real. Truly there are two Worlds now. The real World is where you spend most time, where you have the most connections, the most friends, hold the most influence, develop the most experience, and where you feel most like yourself.

For some of us, the real world is the sky, the streets, the city. For others, the real world is much bigger, much more exciting, and holds way more potential. And as a teenager you can make much more money there too.

Don't blame it on TIM*

Who is responsible for information security within your organisation?

The obvious and rather short answer is that everyone is responsible. From the CEO to the Board to the call center operatives to the interns to the kids on work experience from school, if that still happens.

Some are more accountable than others, some have a clear legal responsibility, and everyone should consider themselves to be part of a concerted normal practice of digital security. Especially the 'lower level' employees, the people who are probably most aware of problems such as weak passwords, lack of encryption, overly accessible folders of clients information, and so on.

Try MBWA. Managing By Wandering Around. If you want to really find out what your companies digital vulnerabilities are, you could do a lot worse than asking the people who use the systems every day.

Copy in the same attitude that everyone in an organisation is responsible for customer service. They're interrelated; digital security is a clear component of customer satisfaction. Just ask any telecoms company dealing with the fallout from not fully appreciating this. The risk to customer satisfaction levels, if your customers account details are stolen by criminals, is absolute.

Bottom line, organisations need to train all staff in basic digital security, and have a system in place for reporting vulnerabilities within individual departments and keeping everyone informed if and when new threats emerge.

It's not difficult, it's not extra ordinary, it's part and parcel of business in 2016.

Otherwise, if responsibility is siloed to a specific individual or department, the defacto consequence is that other people and other departments are not responsible, and therefore inadvertently make life much more difficult for T.I.M, or whoever is to blame when it all goes pear.

LAW. PAINFUL BUT NECESSARY

Cyber Security Regulation in the UK – an overview

Cyber security is concerned both with the security of cyber space (which can include physical places as well as purely virtual ones) and the security of entities that use or rely on cyber space. Entities that use cyber space need to be cyber secure; not simply because of the obvious business impact and reputational issues arising from security breaches, but to ensure they comply with their legal duties.

The law governing cyber security is somewhat of a complex (and dare I say it unintentional) amalgam of various pieces of legislation enforced by a number of regulatory bodies who do not necessarily act in concert. Currently, the only legislative obligation for cyber security is found in section 105A of the Communications Act 2003, which regulates telecomms companies and ISPs. However, the security provisions (seventh data protection principle) of the Data Protection Act 1998 have been interpreted (and enforced) by the ICO to include cyber space and to contain a duty for cyber security ie to protect personal data from cyber security vulnerabilities, including cybercrime. The Financial Conduct Authority (formerly the FSA) is also active in the regulation of data security using its powers under the Financial Services and Markets Act 2000 to police cyber security in relation to FCA regulated entities.

However, there is new legislation on the (not very distant) horizon. The Directive on Network and Information Security, colloquially known as the NIS Directive or the Cyber Security Directive will create a legal duty for cyber security for various public administrations and market operators, requiring them to take appropriate technical and organisational measures to manage the risks posed to the security of the network and information systems which they use and to notify incidents (ie breaches) to the authorities. New national Regulators for cyber security will be appointed with significant enforcement powers. And infrastructures to coordinate national and EU responses to threats, risks and incidents will be created.

The purpose of the Directive is to ensure a high common level of network and information security (NIS) within the EU. The Directive is not yet finalised, but as it is the final trilogue negotiations stage it is now a case of 'when' not 'if' it will be passed. One of the most important issues to be ironed out in the on-going trilogue negotiations concerns the range of market operators who will be under the duty to be cyber secure. However, critical infrastructures and services in the energy, transport, financial services, health and financial services sectors are will very likely be subject to the new regime.

The impact of the Cyber Security Directive and the new EU Data Protection Regulation on your cyber security obligations is significant and both are likely to be passed (in the author's view) in early/mid 2016 and be effective two years thereafter. Therefore, cyber security plans must become a priority for all organisations and in particular for boards of medium to large sized organisations. Those at the very top need to recognise the real risks facing their businesses (and them personally!) and take steps now to minimise those risks by preparing more fully for breaches. What should you do? Start by implementing a detailed cyber security plan with adequate systems, safeguards and processes –and test it regularly. You should also draft, implement and road-test a data breach, crisis and notification policy.

There is significant legislative change looming for cyber security in the UK and across the EU. If you are caught by it, it will have significant legal, commercial and operational impact on your organisation. Do not delay - start gearing up to manage it now. The clock is ticking...

CRAIG RATTRAY

Partner, Gateley Plc

Craig is a London based commercial partner at law firm Gateley Plc and he is technology, payment services and data protection specialist. He advises customer and supplier clients across multiple industry sectors (including financial services) on complex commercial transactions including IT and business process outsourcing projects. He has specialist payment services expertise and the regulatory compliance environment that governs payment services in the UK, including the payment services and e-money regulations and the Data Protection Act.

TECHNOLOGY

Breach response

People expect large organisations, such as telecoms firms, with huge resources at their disposal and leading edge technology, to be amongst the best equipped to keep cyber criminals at bay. However, the fact that high-profile breaches continually come to light, shows that no organisation is immune from attack. It only needs an unwitting employee opening a suspicious attachment, plugging in a USB stick or making a simple error during a routine system admin task and systems can instantly be at risk.

Attacks can come from just about anywhere at any time – whether it is a bored teenager or an organised criminal targeting data for profit. The recent TalkTalk web site breach was a perfect example of the former, where a relatively simple attack was used very successfully, to devastating effect.

Targeted attackers are often far more focussed on their intended victim and better resourced. They have a huge asymmetric advantage over the victim, who has no way of knowing the timing of an attack and has multiple potential vectors to defend.

The reality is that many businesses, not just telecoms firms, maintain vast amounts of personal information, which is highly prized by cyber criminals and is increasingly difficult to protect.

The greatest challenge is that an attack is not noticed quickly enough. The time to detect an attack can stretch to over 200 days, which is too long to be exposed to any type of threat. Conversely, in the TalkTalk example, the breach was detected relatively quickly (within only a day or so). TalkTalk reacted quickly, which should have put them on a much stronger footing to deal with the crisis. However, despite the speed of detection there was still uncertainty around the scale of the breach and the number of subscribers affected. Hence initial PR announcements slightly missed the mark and the level of initial interest (and criticism) reflected this.

As with other past breaches like Target, Sony and OPM; TalkTalk provides valuable lessons. The first and most important step to take following the discovery of a breach is to establish which systems and data were compromised and determine the nature of the attack; both rapid detection and early understanding are vital.

When it comes to leveraging actionable intelligence; information quality and timelines matter. Security teams require integrated security solutions to achieve this. True cyber resilience means appropriately scaled and competent technologies and processes that meet threat levels and response requirements, rather than just point solutions that focus on low-level threats or specific vectors that hackers navigate around to find a "weakest link".

Security functions are increasingly identifying new sources of threat information, all of which needs to be aggregated, digested and investigated to mitigate threats. Increasingly the mass of information requires automated analytics and decision-making technologies to fasten the process, limit the time at risk, remove false positives and enable analysts to focus on threats that pose an actual danger.

Cyber resilience means fit-for-purpose monitoring to identify indicators of compromise, behavioural anomalies or suspicious activity. The automated collection and processing of information allows security operators to make prompt and confident diagnoses and decisions, and to deal with the noise generated by modern IT systems and security controls. Applying the latest in Automated Threat Verification technologies to identified threats allows the minimisation of false alarms and rapid identification, isolation and remediation of systems impacted by an attack.

PETER WOOLLACOTT

CEO & Co-Founder, Huntsman Security

Peter Woollacott is the CEO and founder of Tier-3 Huntsman, and the driving force behind its success. He is an expert in cyber risk and security solutions for enterprises that are serious about preventing, detecting and managing cyber threats. He is regularly sought for advice on ways to use technology to reduce risk, improve governance and, ultimately, deliver competitive advantage.

Huntsman Security is a cybersecurity specialist focused on real-time security detection, verification and resolution in mission-critical security environments, national intelligence, border protection, banking and infrastructure globally. It proactively detects indicators of compromise and allows companies to quickly resolve issues.

COVER STORY
Cyber Security

by BIRD LOVEGOD

"Can I take your card details, please?"
A look at call centre vulnerability

The vulnerability starts when customers give details over the phone. This includes credit cards and debit cards, possibly bank account details for direct debit purposes.

The customer has at that point lost control of their information.
It's a trust-based transaction, and like any trust-based relationship, there's a risk of breach. Some of these call centres are offshore, further complicating the situation in terms of compliance, law enforcement, and so forth. The non-UK call centre employees are earning as little as £200 per month in some instances, and recruitment practices may not be as thorough as one would hope. In the UK, call centre employees are paid an average of less than £16,000 per annum and can be on zero hour contracts. The temptations are huge, and according to Strathclyde Police "approximately 10% of Glasgow call centres have been infiltrated by organised crime".

Even if the call centre is trusted, and the individual operatives are all honest, hacking into the actual phone lines, or the database of call recordings 'for security and training purposes' would give absolute access to the card data. There's always a weak point. It's about accepting that, and strengthening each point in the chain.
And whist the message is usually that the customer is not the victim, it's the card company that loses money, this is only theoretical and not always accurate. The credit card companies are responsible for reimbursement, but not if it's a debit card, and certainly not if it goes unnoticed by the customer for more than 3 months. In addition, the complete card details can be sold on, and can even be used to purchase illegal items from the dark web, further exposing the legitimate holder to a completely new area of risk.

The risk to the brand:

One incident can damage the public's relationship with the brand. Even a single instance can go viral on social media, it depends on who the individual is, how many twitter followers they have, their facebook connections, and how bad a day they are having. The brand loses control once the incident is on social media.
If multiple instances occur, it will be picked up by mainstream media, gathering detractive attention in a snowball effect in a very short period of time. If the brand doesn't have a pre-determined response strategy for this eventuality they will be reactive, and damage limitation is unlikely to be effective.

If a systematic and professional criminal abuse has occurred, things can get really tricky. An example could be a rogue telephone operative concealing a microphone on their person to record every conversation they had for a month. Or a hacker 'harvesting' a database containing card data.
This would almost certainly result in high profile investigations by law enforcement agencies, possibly cross boarders, multiple regulators, multiple lawsuits, merchant claw back, and literally years of customer service repair work, litigation, and reputational repair. Investigation and remediation costs can run into millions – Talk Talk admitted to costs of £35m - plus consequential loss of reduction in new sales, loss of market value – Talk Talk's share price has recovered to 'only' 16% off its pre-data breach price - and loss of senior management expertise if heads are required to roll.

But TalkTalk is the tip of the iceberg. The Home Secretary recently said that "90% of large organisations suffered an information security breach last year" and, according to the UK Government's Department for Business Innovation and Skills "14% of respondents took more than a month to detect their worst breach of the year."

Over to Compliance3 for their commentary on the matter:

Recent consumer research conducted by Compliance3 has found that, in the event of their data being compromised, nearly 40% of people would tell everybody they knew, with a further 16% adding that they'd spread the bad news on social media. And 41% of people surveyed said that they'd never buy from a compromised brand again.
The potential reputational damage and revenue losses are commercially significant. Above and beyond the immediate consumer backlash, the secondary and related impact could be devastating. Modelling only 1st and 2nd generation connectedness and making some realistic assumptions on consumer behaviour, Compliance3 estimates that for every one person that has their data compromised, up to 50 connected people might well change their purchasing behaviour or relationship with a brand as a result of a breach. Multiply this by ARPU (average revenue per user) and potential customer lifetime value, and the true potential impact could be many times more severe than initially estimated.

Compliance3 helps the call centre industry to deliver compliant customer contact. By deploying solutions where customers 'key' their card data into their phone so the agent never hears the card details (not even the keypad tones), we can then help companies protect customer payment card data. We can also help move any existing call recordings to a secure facility and 'cleanse' card data from recordings if they need to be accessed – for regulatory purposes, for example. For one client, we moved over 13 million call recordings off-site, and no card data now enters their environment.

According to Strathclyde Police "approximately 10% of Glasgow call centres have been infiltrated by organised crime".

RISK

Cyber Crime Risk Management

by Marios Kyriacou, Managing Director at MNK Risk Consulting

Cyber crime is just another type of operational risk. In fact it is included in the operational risk event types defined by Basel under External Fraud. External fraud and cyber crime risk can be managed through the implementation of a risk management framework that relies on the following components:

- Risk and Control Self Assessment (RCSA)
- Capturing and management of historical risk incidents related to cyber crime
- Scenario Analysis using external data of similar incidents occurred to peer institutions
- Setting up a Key Risk Indicator monitoring program
- Modelling the occurrence and loss severity of cyber crime risk.

Managing Historical Risk Incidents

An incident is broken down into three elements: cause, event, effect. Recording historical incidents on cyber crime risk means understanding the event, which factors have led to that event and its financial or other impacts. Institutions should maintain internal incident databases using a preset taxonomy. Recorded cyber crime threats could be categorized into the following event types, Human error, Theft/Loss, Insider Misuse, Social, Malicious Software, Hacking, Product flaws.

Once events have been identified with respect to their type, the analysis of the cause and impact follows. The cause of events is necessary if a manager wants to track down the root of the problem in a business process; preventing other events with similar cause from occurring in the future.

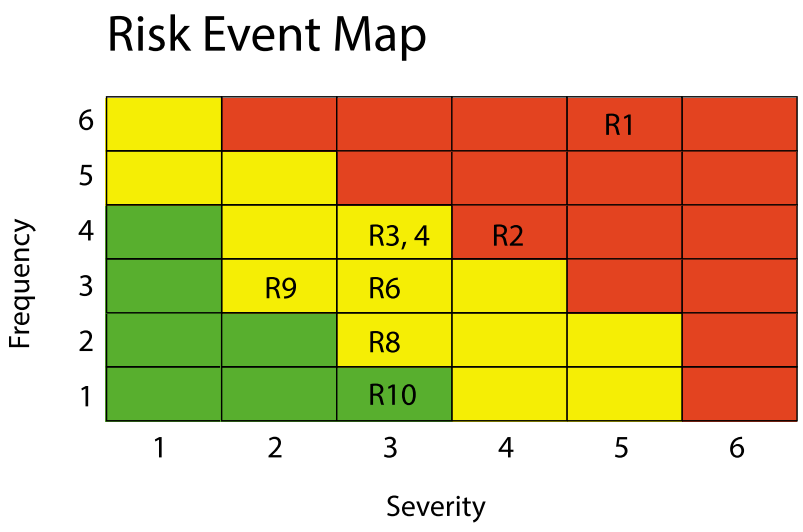
Managers need to prioritise the types of operational risks they should manage and mitigate. The ranking of risks would depend on the financial impact, and or other indirect impacts such as reputational damage.

Incident statistics such as the single most severe loss event, the total loss amount per year, the most frequent cause, and the top-ten most severe events enable management to identify any patterns and have a better understanding of the risk profile. In addition it helps the Risk Manager to initiate corrective measures, follow up on their timely implementation and monitor their effectiveness.

Potentially disastrous scenarios could be identified using internal incident data as well as external actual loss data; the latter may be sourced from either commercially available public loss databases or industry-pooled consortia (e.g. the Operational Riskdata eXchange Association ORX).

Key Risk Indicators (KRIs)

KRIs are dynamic data indicating the level and trend of specific risks. They focus on the significant risks which typically emerge from the analysis of RCSA results, historical cyber crime incidents and scenario losses described earlier. For example, with reference to the ten risks depicted in the heat-map below a Risk Manager could assign KRIs for the two risks (namely R1, R2) which scored high.



Modelling cyber crime risk

There are two stochastic processes that drive the measurement of cyber crime risk: the severity of losses and the frequency of events. Compounding these two stochastic processes results into the simulated distribution of possible future annual losses from cyber crime risk. From the simulated annual loss distribution one can then derive risk measures such as the annual Expected Loss (EL), the Value-at-Risk (VaR), and Expected Shortfall (ES). EL arises on a continuing basis in the 'normal' course of doing business and as such could be absorbed through P&L either by provisioning or (risk based) pricing. VaR looks at unexpected losses, whereas ES at catastrophic losses. Unexpected losses, although unusual, still need to be anticipated and covered through Tier 1 and Tier 2 capital reserves. Catastrophic losses (which are the largest in size of the unexpected losses) could be covered by insurance or other risk transfer techniques.

INSURANCE

DOES FINTECH NEED CYBER INSURANCE?

SIMON GILBERT

Managing Director,
Elmore Insurance Brokers Limited

"There are only two types of companies: those that have been hacked and those that will be. Even that is merging into one category: those that have been hacked and will be again." Cyber attacks are coming thick and fast and becoming almost an inevitability for UK business. It is as FBI Director Robert Mueller foresaw when speaking in March 2012. Ignorance is no longer bliss. It is essential fintech firms proactively manage their cyber risks, which means making a decision whether to purchase a cyber insurance policy.

Ashley Maddison, the US Office of Personal Management, Carphone Warehouse, Lloyds Bank, TalkTalk, M&S, and most recently Vodafone are just some of the cyber security breaches that have occurred during 2015. UK businesses in the fintech industry will be feeling particularly vulnerable wondering if they will be next. Recent events serve as a strong reminder as to the importance of regularly reviewing cyber security arrangements. The board of directors must ensure they understand the most recent threats and are suitably prepared in the event of an attack, or shareholders may hold them accountable.

CYBER INSURANCE EXPLAINED

Typically, the cyber insurance industry breaks a cyber event into three parts: Event Management, Financial Loss and Liability.

Event Management involves the internal and external expenses of managing the response to a cyber event. Cyber insurers vary in the extent of cover provided in Event Management, but in general they recognise that providing access to third party cyber security experts can mitigate the consequences of a catastrophic event.

This is sometimes spearheaded by a cyber response coach, an industry expert responsible for advising a business on how to handle and manage a cyber event. Typically this will start with an investigation by third parties to establish the extent of the issue. If card data is compromised then insurers can indemnify the costs arising from a specialist PCI Forensic Investigator (PFI) investigation. Consultation on how to manage legal and regulatory issues will also be covered as well as a crisis communication strategy. Establishing a call centre to field queries and providing credit monitoring are the last elements of cover.

Financial Loss takes into account the increased operational costs and reduction in profits as a result of the attack. This is known as non-physical damage business interruption, and is typically excluded from property insurance. Should any fines and penalties be issued by regulators (Information Commissioner's Office) and industry associations (for the loss of sensitive card payment data), then cyber insurers will cover this with the proviso that these are insurable by law. Costs in managing a cyber-extortion situation — and the ransom itself — can also be covered.

Liability tends to impact some months later. Affected individuals or businesses may bring claims or written demands for failing to protect their information. They may seek compensation for financial losses from hacking, or damages from identity theft. In cases where customers are claiming from multiple jurisdictions, cyber insurers can contribute towards defence costs and any resulting damages from multi-jurisdictional claims.

THE RISK OF GOING UNINSURED

Many fintechs are running a great deal of cyber risk on their balance sheets. By effecting suitable cyber risk management, such as a robust cyber security framework, including penetration testing and effective threat detection through multi-layer monitoring, many cyber attacks can be stemmed from an early stage. An incident response plan, which considers not just business continuity and disaster recovery, but also easy to implement steps and pre-contracted responders, can make the difference between a disastrous impact to reputation and a positive outcome for the entity in question.

Elmore Insurance Brokers Limited advises its fintech clients to actively manage risk to manage down premiums. Insurance is a partnership between businesses and insurers. This partnership can be significantly enhanced by focused engagement to understand and implement information security risk management best practice, which includes cyber insurance.

SUMMARY OF A CYBER INSURANCE POLICY

EVENT MANAGEMENT	FINANCIAL LOSS	LIABILITY
Incident response consultation	Loss of net profits	Privacy defence costs and damages
IT forensics (including PFI costs)	Increased costs of working	Failure to notify defence costs and damages
IT professional services	Reputational loss	Hack or virus defence costs and damages
Legal & regulatory consultation	Regulatory fines & penalties	Defamation defence costs and damages
Notification management	PCI Awards	IP defence costs and damages
Crisis communications	Extortion expense and ransom	Media content defence costs and damages

Source – Financial Lines Department, Elmore Insurance Brokers Limited

BACKUP FOR YOUR BACKUPS

JAMES YORK

James is the Founder of Worry+Peace, the modern insurance store and concierge.

The rise of relevance for Cyber insurance

It seems you can't click or flick a page these days without seeing a nightmare tale about a hack or cyber security breach. According to a recent government report, 81% of large businesses and 60% of small businesses suffered a cyber security breach in the last year, and the average cost of breaches to business has nearly doubled since 2013. How, if at all, should you protect your business?

Firstly, try and have a policy — explore the guidance of standards like ISO/IEC27001. For most of us, though, Cyber Insurance should become as common a purchase for UK businesses as property insurance within the next 10 years. Don't take my word for it, that's according to the Association of British Insurers.

Who should be buying it? If you're reliant on cloud services, run a cloud service, keep hold of Personally Identifiable Information for customers, or data from payments - this should already be on your radar. Beyond that, these products often cover the very real risks associated with using social media and content marketing - defamation, copyright and IP complaints. Surprising to many a blogger, I'm sure.

Fortunately, not only is the UK home to the second-fastest growing startup ecosystem, it's also home to the third-largest insurance market in the World - well stocked for such a need. Our insurers currently underwrite a whopping 10% of the global cyber market.

Plug alert: there's quite a range of choice brewing. My brand, Worry+Peace, soon launches a panel accessing (directly/through wholesale channels) most of it. According to that same government report I cited, there are about 13 major carriers in the UK looking at this class.

It's not always expensive, either, prices can be from as little as £150. Be warned, though, because it's quite a new product range, the applications can take longer than others to fill out. Have a cuppa ready, or a nice broker to fill them out with you.

So, what's the global worse case scenario? There's a way the insurance sector checks it has all bases covered — realistic disaster scenarios stress test their ability to cover a mega-bad thing. Their estimate for a Cyber "RDS" is about £20bn. Currently, the market reckons it can muster circa-£60bn if needed to cover broader RDSs. That's a pretty sizeable context for a little-known class of insurance — Cyber. Makes you think, I hope.

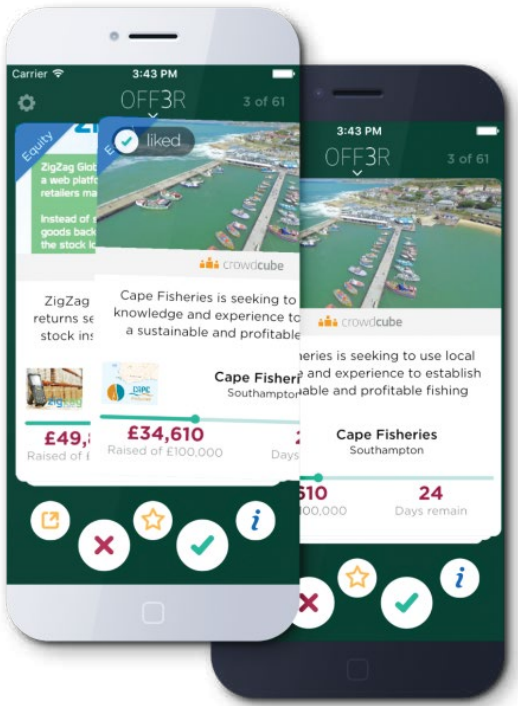
Visit Worryandpeace.com/cyber to find out more about Cyber Insurances.

OFF3R

The world's first mobile crowdfunding aggregator

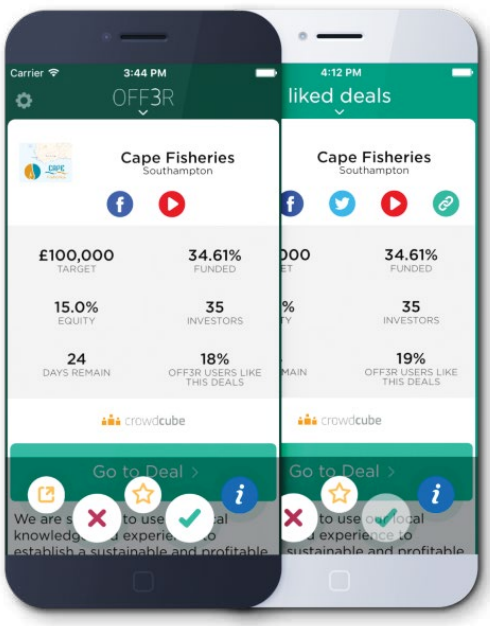
It is a critically acclaimed mobile app that aggregates deals from over 20 of the leading crowdfunding platforms. The app uses a swipe user interface to make it simple and enjoyable to browse deals, watch pitch videos and digest investment opportunities about exciting companies.

It's the best way to discover and track deals across platforms. You can also enable alerts and notifications to stay up to date with your favorite opportunities. OFF3R does not make any recommendations. It is purely an information service that collates publicly available information into a mobile application.



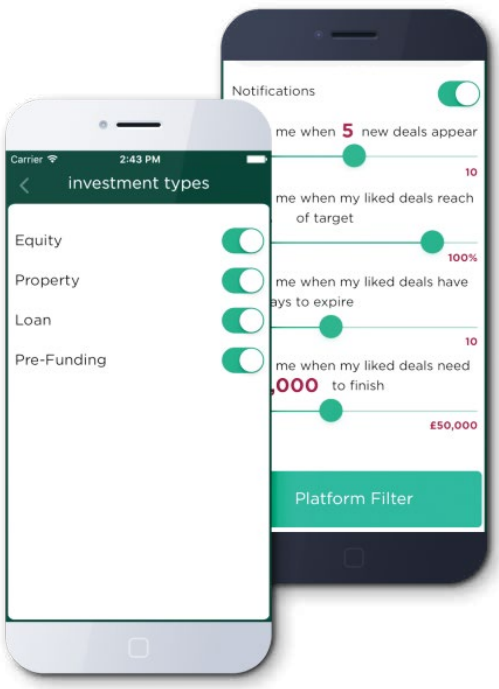
DEALFLOW AT YOUR FINGERTIPS

OFF3R displays a brief overview for each campaign, flip the card to see more. Digest each deal card and swipe to sort.
It's free and quick to sign up to OFF3R. Swipe right if you want to track a deal, left if you want to dismiss it or click on the star to add it to your favourites.



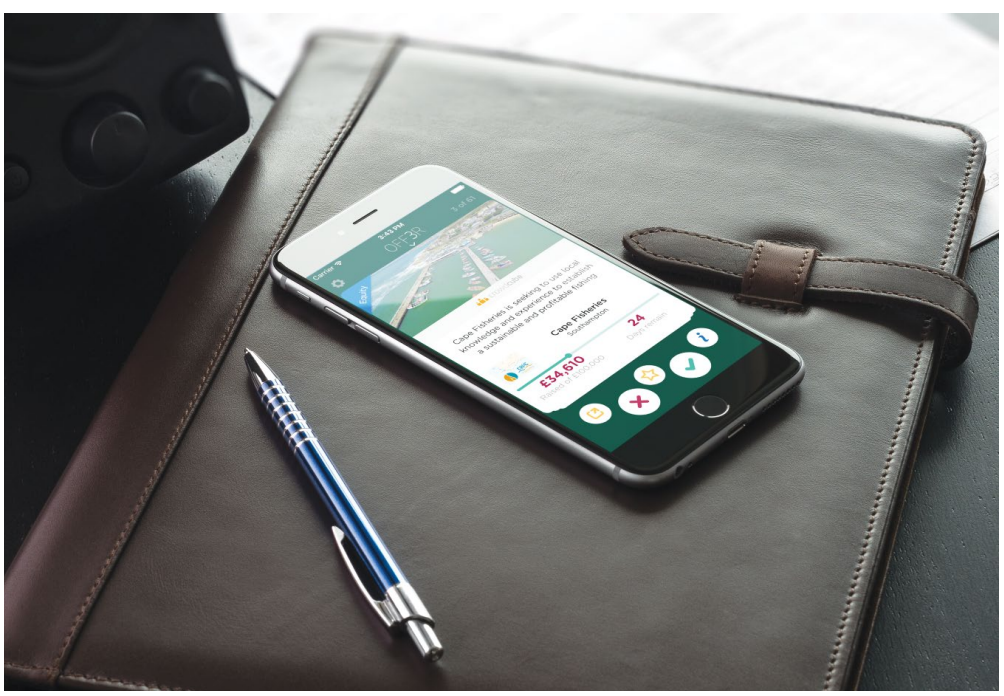
DETAILED

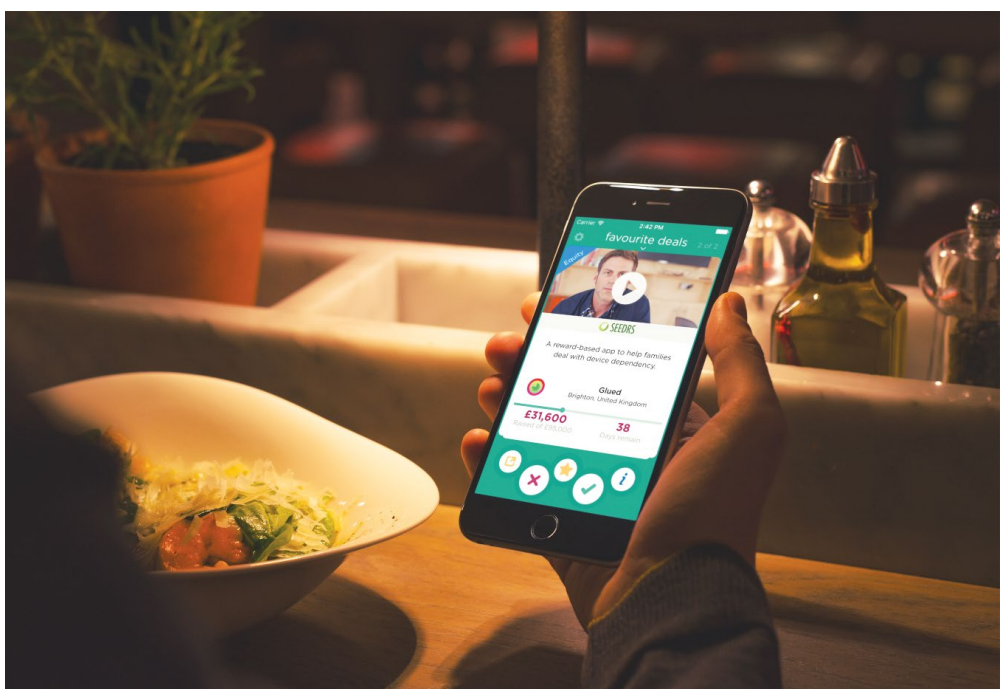
Flip the deal card over to see more information on the deal and visit the deal pages on partner platforms.
Access leading crowdfunding platforms in the palm of your hand ensuring you'll never miss an opportunity.



PERSONALISED

Tailor notifications to ensure you don't miss an opportunity. Set new deal alerts and stay informed when your selected deals are reaching their target or their closing date. Filter the platforms and the type of investment opportunities you want to see.
Manage your dealflow.





Platforms

ANGELSDEN

The platform is an angel-led crowdfunding platform where angels and sophisticated investors invest in small to medium sized enterprises. Angels Den's approach means that once an 'anchor' investor is on board, the funding round is then opened up to the crowd. This gives the crowd the luxury and confidence of investing alongside an experienced angel investor. 94% of funded deals on Angels Den are still trading identifying a niche for investors that add value to the startup business. Their top performing sectors are Technology, Food & Drink and Consumer products.

crowdcube

The platform is now one of the biggest in the UK with a constant deal flow of equity and bond investment opportunities. The founders wanted to give entrepreneurs the opportunity to take control of raising funding from their own network of friends, family, customers and strangers. Crowdcube aims to give people the chance to become an 'armchair Dragon'. The platform itself has over 225,000 investors signed up and have successfully funded 324 companies. Companies using Crowdcube have raised over £115 million since starting and the platform operates a direct investment model where investors invest directly with the company that is fundraising.

eureeca.com

Eureeca was the first global investing market place. The platform is based in the United Arab Emirates and is focussed on startups that are seeking funding in this region. The platform launched in 2012 and allows investors to invest from as little as $100 per investment in a wide range of businesses.

CrowdLords

CrowdLords are directly connecting investors and property professionals so that more people can benefit from investing in property. They want everyone to be able to invest and benefit from property investment without the traditionally high cost barriers to entry. A core concept of the platform is that by pooling resources more can be achieved.

INVESDOR

Since starting in 2011, Invesdor set out to achieve their vision of becoming the leading equity based crowdfunding platform and offer the best investment opportunities across Finland, Sweden, Estonia, and Denmark. The Invesdor team specializes in equity-based opportunities but has also recently introduced bonds on to their platform. This leading European platform offers investors the opportunity to invest in a market outside of the UK.

SEEDRS

Seedrs has become a leading crowdfunding platform in the UK by offering a nominee model to their investors. This means that Seedrs acts as legal shareholder on behalf of the investor and that you will have the same rights however big or small your investment is. Seedrs shows equity and bond investment opportunities and have been backed by a number of high profile investors since they launched. In 2014 they funded 110 campaigns from 20,367 individual investments making them a driving force not just in the UK but Europe as well.

Crowded space

The rise and rise of Crowdfunding provides investors with opportunities to buy into companies at an early stage, across a wide spectrum of sectors.

OFF3R is a simple concept, well executed, and actually quite elegantly designed mobile app that aggregates the offers from crowdfunding platforms into a tinder style swipe format. There are about a dozen UK platforms, and another dozen non UK platforms that can be filtered so you can select exactly which platforms you want to see content from.

It's probably the quickest way to gain an overview on the Crowdfunding industry in terms of companies endeavoring to raise funds this way, determining which tend to be more successful than others, which platforms are better suited to which sectors, and a range of other insights..

For potential investors in these companies, OFF3R is fundamentally a way of shortlisting possible investments, monitoring their funding progress, engaging with the process, reading the submitted business plans and documents and so on.

What you can't do is invest through OFF3R, to actually put money into one of the companies it requires the user to go through the correct procedures on the actual Crowdfunding sites which vary considerably, platform to platform.

For this reason, OFF3R is a support service to the platforms, and the companies on them, rather than a middleman between the investors and the platforms. It's a reassuringly symbiotic relationship, with OFF3R keen to develop and analyse the valuable information and insight that this position allows.

OFF3R as a company will shortly find itself in the interesting position of having detailed historical and real-time insights into the Crowdfunding sector itself, and the multiple sectors that use Crowdfunding to raise capital.

Over the next few years this may become increasingly significant, P2P and equity Crowdfunding are proven challenger systems for business funding, and having an understanding of success and the way success is both determined and achieved, is valuable.

It's going to take several more years, at least, before we start to have sufficient data regarding the live or die rate of crowdfunded companies, and investors should be cautious. B2C business models are seemingly more common, building a user base as well as investors, but B2C apps for example can be difficult to make a successful business from, requiring hundreds of thousands of users to reach viability in some instances.

Where as less familiar but more viable B2B models may find Crowdfunding a more challenging experience.
Horses for courses.

But these are just speculations. The power that OFF3R is aiming for is having the data, the facts, the statisical truth.

Until then, investors just have to follow their interests, insights, intuition, and sometimes the crowd.

OFF3R is not a crowdfunding originator. OFF3R is an aggregator of publicly available information, you will need to register on each platform and agree to specific terms to access additional investment information. OFF3R is targeted towards investors who are sufficiently sophisticated and/or accredited and understand these risks and make their own investment decisions. Investing in early stage businesses involves risks, including illiquidity, lack of dividends, loss of investment and dilution, and it should be done only as part of a diversified portfolio.

REPORT

New research explores consumer attitudes to digital finance

Research by Nostrum Group, a lending technology provider based in London and Harrogate, has revealed that consumers increasingly value personalisation, honesty and integrity ahead of speed and monthly cost when choosing a loan provider. CEO Richard Carter gives The Fintech Times readers a preview of Nostrum's research, unveiled in December.

There were some interesting themes emerging from Nostrum's third annual report into consumer attitudes to digital finance, titled 'Personalisation in Digital Lending'. Our research, which surveyed 2,000 adults, found transparency (84 per cent) is now second only to low interest rates (92 per cent) as the factor consumers consider to be the most important element when sourcing a loan. The third most important factor is speed (73 per cent).

In recent years we've seen the lending industry become ever more influenced by the digitally-savvy consumer, and several factors now point towards an increasing preference for digital lending. Just 14 per cent of those surveyed could remember their last bank branch visit, while 53 per cent of those surveyed now use a mobile banking app.

People are now more willing to accept the role of social media data in loan decisions. 49 per cent of those surveyed aged 18-45 say they are open to the notion of lenders using social media as a means to make credit decisions. This represents a significant increase on the 40 per cent of the same age group who expressed a positive response to the same idea in 2014.

The challenge to banks and other lenders is not just to provide lending facilities digitally. To appeal to existing or potential customers they need to be honest, transparent and able to provide a personal experience, all with a competitively priced product.

Digital finance has arrived

Our survey found general indifference to questions about technology in finance, which in previous years have bought stronger reactions. This in combination with the ubiquitous presence of smartphones and increasing market penetration of tablets and mobile banking apps confirms that consumers have stopped viewing digital lending as the future, and are increasingly comfortable accepting it as part of their day to day lives.

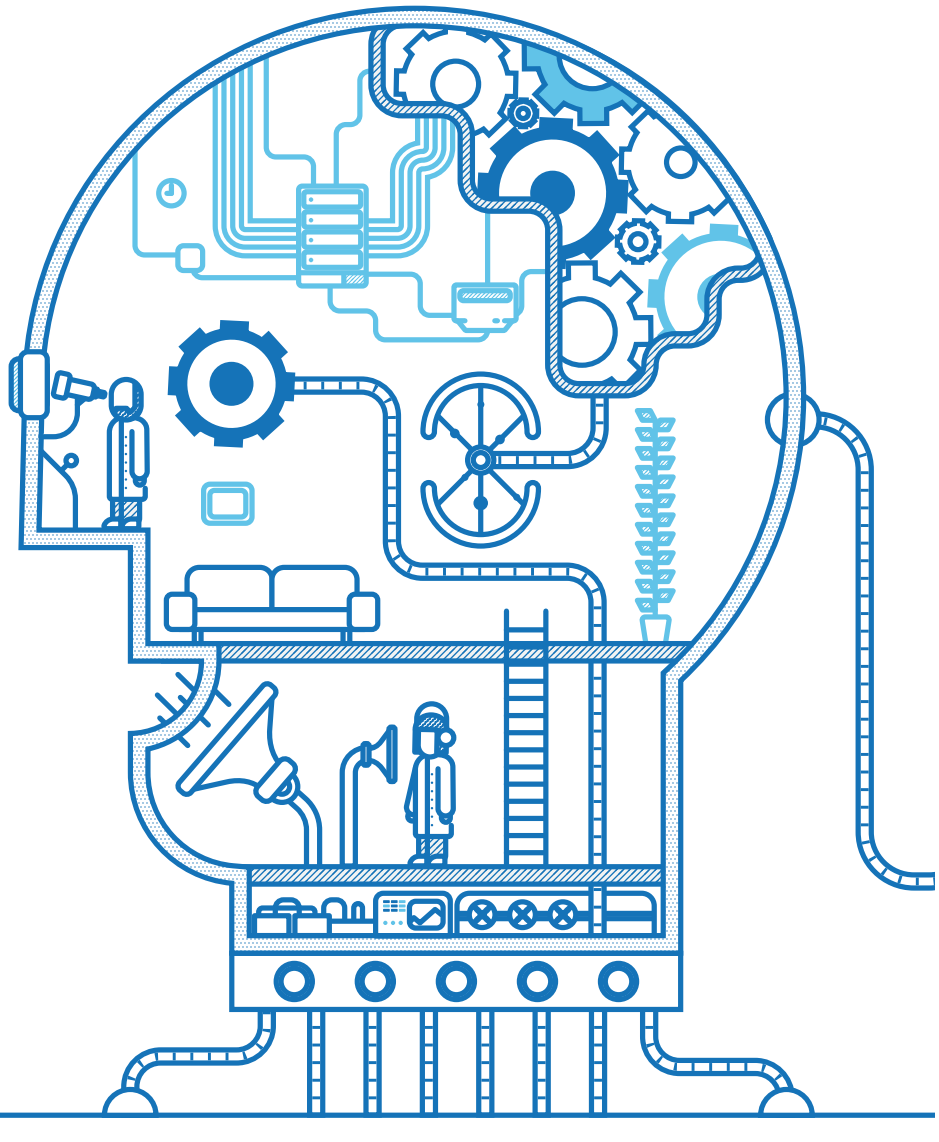
We see this as an opportunity and a threat for existing banks and lenders, as it makes potential market entry by some of the biggest tech and social brands ever more plausible and likely to succeed. The strength of the current consumer credit industry lies in experience but the market faces unprecedented change in the coming years, and technology has revolutionised the way consumers can be serviced. Whether one single company can meet these demands remains to be seen, but to compete the industry needs to take a long hard look at itself and not be afraid to completely rethink the way it operates.

The future certainly looks bright for digital lenders. There is market share still to be acquired from high street banks and if consumer affordability continues to be strong for the majority of 2016, if not all of it, retail point of sale finance operators could benefit from more spending on the high street.

Personalisation in digital lending

Creating a personal touch and operating in a way that resonates with the consumer's own core values offers an opportunity to differentiate in an increasingly busy marketplace. Banks and Fintech innovators are likely to be pleased to see customers acknowledging the role social data can play in underwriting. This may represent a recognition that consumers acknowledge their personal data will need to be shared in order to receive a higher degree of customer experience. At the same time, it indicates that if the lender is deemed trustworthy, providing this data will not be a huge issue.

So what can we conclude from this research? It seems the perfect platform for innovation in digital finance to bloom has been set, building on increasing confidence in digital transactions and demand for credit of all varieties.



NOSTRUM GROUP

REPORT

2015 Fintech Disruptors Report STARTUP Banking

By MagnaCarta

The consequences of the financial crisis of 2007 – 2009 were far reaching. They are still being felt today – the difference in European output in the second quarter of 2015 compared to that predicted by pre crisis levels is equivalent to the size of the German economy.
For established banks the complex array of challenges that are confronting the industry, and helping to level the playing field as a result, mean that in many ways banking – both old and new – is in 'startup' mode.

The Fintech Disruptors report identifies and discusses seven inter-dependent themes, outlined below.

The full report is available from MagnaCarta Communications. Thank you to The Dock, London, for hosting the release event.

SIMPLICITY

Easier access to consumers through digital channels, and specifically smartphones, is driving the trend to straightforward products distributed by new fintech entrants, in most cases themselves simple, single product companies. While this strategy may be impractical for multi-channel institutions, the research highlights the opportunity for banks to simplify the user-experience, rationalise product lines and improve returns, which now stand on a level comparable to utilities companies.

TRUST

Trust, once a byword for financial services has been severely damaged by the financial crisis and waves of scandal in the decade following it. Loss of trust has opened the doors to new fintech, non-bank competitors. While most of these have not yet been tested by a downturn, waiting for the next crisis to restore trust is not a viable option. The report shows that winning back customer trust will require an emphasis on re-building the relationship with consumers through transparent pricing and communications, and greater use of technology to replace human interaction with automated systems.

AGILITY

Smartphone app use has radically altered consumer demand for innovation, with new products launched more quickly, tested in the open market and continuously refined. Organisations in this report underline how banks are adapting to this cultural change with innovation initiatives that include venture capital investment, internal development and acquisitions. Most critically however, greater collaboration with third parties outside the bank and, paradoxically after a wrenching financial crisis, 'getting over the fear of failure' are increasingly viewed as essential ingredients to an agile innovation strategy for large institutions.

RELATIONSHIP

The focus on user experience by fintech entrants, including those in this report, is drawing attention to the opportunity to redraw the relationship of financial services providers with their customers. For banks, this will mean seizing the potential to leverage deep pools of data for greater customer insight to understand how to monetise their services transparently in a way that fosters the longerterm relationship.

TRANSPARENCY

The price transparency enabled by the first internet wave at the beginning of the century, in the form of price comparison sites such as Moneysupermarket.com, has been complemented by an influx of new entrants with straightforward pricing and simple business models in the age of the mobile internet. For banks, often characterised by complex businesses and opaque pricing, a response will require a root-and-branch commitment to transparency to help restore trust and re-build the connection with customers.

UNBUNDLING

New fintech entrants are exploiting the advantages of single product focus, following a trend that was set by the launch of mono-line credit cards in the 1990s. The benefits this strategy affords include greater emphasis on the customer to build loyalty and a simpler corporate and revenue model. With fintech valuations riding high, countering this threat solely through acquisition is probably unrealistic. To compete, banks will need to develop a clearer understanding of how to leverage their multiple channel structure to create a better experience and deliver greater benefit, while exploring the potential for unbundled product pricing.

PRICING

The impact of the fintech revolution on product price-setting of products remains the most unresolved area of the ongoing shake-up in the financial services industry. Price is already the primary battleground on which the challenge to existing incumbents is being fought. The research reveals that while transparent pricing is a central pillar of the strategy for new entrants, banks and complex financial services organisations are trying to understand how to reconcile consumer expectations for cheaper digital products with an obligation to maintain multiple delivery channels.

GLOBAL
Israel

Israel: From Startup Nation to Cyber-Security Nation

If you've been to Tel Aviv recently, you've most likely heard local entrepreneurs refer to Israel as "Start-Up Nation." This name was coined by two American journalists who, in their 2010 book, explained how Israel turned so hi-tech-heavy (hint: skilled immigrants & mandatory military service).

But what you may have missed is Israel's rapid transition from "Startup Nation" to "Cyber-Security Nation," a transition that has produced a wealth of opportunities for angel investors, venture capitalists, and global corporations such as McAfee, Microsoft, IBM & PayPal, who have begun seeking acquisitions in the country.

In the last two years alone, CyberArk IPOed at USD 500 million (it is traded today at USD 1.2 billion); IBM acquired Israeli security startup Trusteer for USD 800 million, and Microsoft acquired Aorato for USD 220 million and Secure Islands for USD 150 million. To name just a few exits (there were many, many more).

Israel's journey to the forefront of cyber-security innovation dates back to the founding of CheckPoint by Gil Shwed in 1993. Shwed, who was then a 25-year old graduate of the 8200 Elite Technology Unit of the Intelligence, recruited his army "buddies" to become the first employees of the company.

CheckPoint's success as the inventor of "Stateful Inspection" or the "Firewall" created a domino whereby the CheckPoint founding team spun off to create their own companies (Imperva & Palo Alto Networks). These successful security entrepreneurs became active angel investors, thus creating a "virtuous circle" in the Israeli security ecosystem.

Fast forward twenty years, and the CheckPoint Domino Effect has given birth to over 300 security startups in various cyber-security domains, including industrial cyber-security, web application security, user behavior analytics, biometric authentication and even car cyber-security.

Israel's booming cyber-security ecosystem, which attracted as much as 11% of global funding and produced over USD 6 billion in sales in 2014, has been driven largely by an unusual supply of talent that comes out of its top military units. Shwed's 8200 unit is just one of those units; others include the Cyber-Security Unit and the Software Unit.

These military units pre-screen and train young high school graduates to become tech leaders. At 18, these guys and girls confront complex technological tasks that have real-life implications, to say the least. The structure of these units is unique to the extent that they are often non-hierarchical and welcome the critique of younger members. In effect, these units operate almost exactly like startup incubators.

One of Israel's most fascinating contributions to cyber-security innovation is in industrial cyber-security.
The domain of OT (Operational Technology), as opposed to IT (Information Technology), has seen the rise of a few very successful Israeli startups in the last couple of years. These startups' uniqueness is their ability to connect to industrial networks in a non-intrusive manner and detect anomalies in the network. In light of the rise of industrial connectivity both in the US and Europe, these Israeli startups have attracted a lot of investor and customer attention.

Another Israeli forte has been in User Behavior Analytics, an emerging field in the cyber-security space. Israeli startups have learned to correlate log data with active directory data in a way that automatically points to rogue or suspicious users (employees) in a company. Considering that 82% of cyber-attacks involve stolen user credentials, these startups have grown incredibly fast.

Israel only is 3.5 hours away from Europe, and the wealth of security innovation found in a few square kilometers in the country is simply unparalleled. As global connectivity rises, Israel will continue to produce some of the world's most innovative and protective state-of-the-art cyber-security solutions.

SHIRA KAPLAN

CEO & Founder, Cyverse

Shira Kaplan is the Founder & CEO of Cyverse, a business development & investment firm based out of Zurich and Tel Aviv that focuses on Israeli cyber-security startups. She is a graduate of the 8200 Unit and Harvard University. She is available at shira.kaplan@cyverse.ch.

GLOBAL

France-UK

French on British Soil: It's not about the money.

MIRA MUDHIR

London is one of the world's largest centres for financial institutions, being home to something like 251 banks, 588 financial services companies, and hundreds, possibly thousands, of emerging fintech. The financial services sector in the UK accounts for approximately 9.4% of the country's total GDP making it one of the largest globally, and more active than any European peers.

However, within the past few years technological progress has forced all governments to turn towards entrepreneurs with a view to attracting or retaining them: clever branding, helpful legislation or increasing propaganda budgets, everyone wants more startups in their town / city / country.

This brought me to La Résidence de France in London. I was attending La French Tech, an event that the Minister of State for Digital Affairs **Axelle Lemaire** announced to be "the world premier of many more to come." During the conference we heard many French entrepreneurs proclaim jokingly that they had not chosen to move to the UK for "tax purposes", emphasis on the NOT. During the Q&A session, the same young entrepreneurs spoke about the difficulty of getting funding in France. This peaked my interest.

Later I asked Lemaire in person: "Why do you think there is a leakage of French talent to the UK? Are there any legislations that will help the advancement of technology in France?" Unfortunately, the answer was unclear. Lemaire's only comment was: "I'm truly baffled that French entrepreneurs are leaving home! It's a lot easier to start a business in France than it is in London. How do we aim to change this? Well... Through you! The media!" Unsatisfied, off I went, to sate my curiosity.

Shortly after, I met **Laure Crémieux**, a 24 year old Parisian contractor, currently freelancing in London for a French corporation, and one of the top global energy players.

I asked Crémieux her thoughts on what she later titled "The French Talent Exodus". Passionately she explained how the initial incentives lure you in, "just for the laws and regulations to choke you." She continues, "Talented entrepreneurs leave France, to the point where some of the country's young business-leaders have started a campaign to woo them and their international expertise back. It's called '#ReviensLéon' named after an 80's TV ad enticing youngsters to eat at home. The target for this year's campaign is the same: youngsters – now all grown up, living away from the homeland."

This point was later reinforced by **Sylvain Girard**, a French entrepreneur and founder of Angus.ai.

Girard had been an expat for many years, and has recently returned to France to start his business. When asked about the benefits of starting a business in France, Girard responded, "It all depends on what stage your business is at. In the early stages of a tech company, France is an excellent incubator. We have many engineers who are, after all, the producers of tech products. They are affordable and highly trained. And because the government aims to support French engineers, you get a tax exemptions in your first year of business. So when the company wants to scale up, or start their search for investment, they tend to move to places like London or Silicon Valley."

French youngsters today take risks, think big, break conventions

"France has never had an entrepreneurship oriented culture". Crémieux and Girard, whom I interviewed individually, answered harmoniously. "The French population is rather reluctant to take any kind of risk. France has always been culturally far from the 'self-made man' ideology. French people have historically had a predisposition toward salaried jobs. Social protection of employees tend to encourage job stability. Hence the "Contrats à durée indéterminée" - the golden legislation that prohibit companies from firing their employees."

Crémieux refers to the recent transformation of this convention brought about by French youngsters. "They are now taking bigger risk, for the first time in 10 years. Partly due to the high unemployment rate of 10.5%, France is seeing an increase in small businesses. Last year a quarter of recent graduates of HEC, an elite business school, have started their own company. That is a significant change as opposed to one in ten, just a decade ago." Consequently, the French startup ecosystem – La French Tech - is growing rapidly. Startup weekends, investment fairs, and international campaigns are emerging everywhere to bring enthusiasm among spirited young self-starters. Crémieux, "The rise of digital sectors is often seen as an opportunity to grow a company without capital expenditure: no risk needs to be taken by timorous French entrepreneurs, all it takes is a computer and time. Finally this trend towards entrepreneurship is enhanced by success stories that show risk-free possibilities."

To quote Marc Simoncini, one of France's most successful web-entrepreneurs: *"Seen from abroad, France is the last country an entrepreneur wants to go to."* Pourquoi?

Crémieux, "Because France has kept its reputation of being an expensive country. Where tax rates are discouraging, labour laws are complicated, bureaucracy procedures are full of obstacles, banks are reluctant to offer credits and venture capitalists do not exist. And this is despite the country's drastic efforts to become SME attractive. The main reason for French companies to collapse remains the lack of funding."

Girard, "I think this is a bit more of a cliché than the reality. You have different instruments to employ people in France. You have many consultant contract laws, which are the same as that of the UK. You have many developers, and PHD's that you can employ at very affordable prices."

Surely, what's drawing French startups to London is not just dire trade conditions in their homeland... Foreign corporations have been controlling 39% of UK patents since 2012. This is far more than the EU as a whole, at just 13.7%. This exceeds the foreign-owned patents in the U.S. (perched at just 11.8%) by 27.2%. Of course, it is no surprise that the UK is the fastest growing region for Fintech investment (Accenture). The UK deal volumes have been growing at 74 percent a year since 2008, compared with 27 percent globally, and 13 percent in Silicon Valley. During the same period, the value of Fintech investment increased nearly eightfold, to US$265 million in 2013 – a rate of 51 percent a year, nearly twice the global average (26%), and more than twice that of Silicon Valley (23%).

This time I was determined to find British expertise on the subject. Thus, meeting **Geoff Graham,** Fitzgerald and Law (F&L), a global exponential advisory firm that works with US and EU tech firms who are looking to expand to the UK. F&L specialises in the taxation and accounting aspects of corporate expansions. The firm sees a large number of French Fintech startups, coming in search of funding. Graham, "Many French tech startups come to the UK when they are ready for their first round of funding, they see the UK as having greater access to funding. From conversations with them I gathered, rightly or wrongly, that London's Fintech sector is far more developed than the rest of the EU."

Surely, funding is not reason enough for so many foreign entrepreneurs to pack their bags and leave their home, friends, and family behind. What other reasons are there forcing entrepreneurs to migrate to Britain?

Graham, "The availability of VC investment is of primary importance. As reported by London and Partners earlier this year, London attracted 50% of all European Venture Capital investments.
Access to mentorships: 36 out of 57 of European accelerators and incubators are based in London, such as Level39 which is renown and very well regarded on a global scale. English language makes it so much easier and cheaper to go global with your company. Which is especially useful when trying to attract American investors. Also with UK laws it is very easy to set up or fold a company."

The UK's leading financial infrastructure, supportive regulations, accelerators and mentorship programs for startups coupled with large availability of capital and English as the main business language - these are all major factors that attract disruptors on a global scale; and not only the French.

LEVEL39

Introducing

Level39

194 really interesting stories to tell

"Level39 provides curated content every week. That means a 'curriculum' offered to all our members, where they can sit down with investors, mentors and advisors for one-on-one sessions which we organise." Asif Faruque

Asif Faruque, Head of Content of Level39, meets, greets, and leads us to the members' club restaurant.

Soft jazz soothes the space, and a choice selection of art softens the walls. I recognise a piece from Kurt Beers' gallery, a mandala, upon closer inspection, one realises the complex geometry is entirely constructed from electrical components, transistors, capacitors, transformers.

Other artworks are similarly digitised. A framed print of a girl, in the style of 19th century portraiture. Her eyes open and move as I approach. Sculptures, a glass sphere, within a triangle, within a cube. The three lit by LEDs, which change colour as I view from another side. I wonder if Kandinsky's colour shape theory has been applied, or if the artists here are leaving the past in the past, and are rebuilding from a new foundation, to leave legacy, not behind, but in the future. A contemplative, innovative, high technology space, with the meditative energy of a dojo. Canary Wharf Group's art curator is Keith Watson, a former gallery owner, and now procurer/curator of digital and kinetic art from all over the world to display at Level39.

Where better to sculpt the very future of finance, banking, and change.

Level39 was formed in 2013, it is of course Level39 of One Canada Square, Canary Wharf. Its Head, Eric Van der Kleij, was the former CEO of Tech City UK, the Government backed organisation designed to bring tech to London. Seems to have worked. Story goes, after he finished at Tech City UK, he went to an event and met Sir George Iacobescu, the chairman of Canary Wharf Group, who said let's bring tech to Canary Wharf, and Eric said sure.

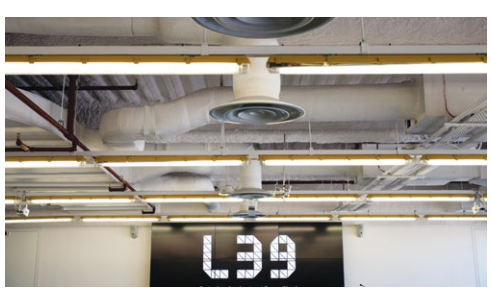
From the windows of our viewing platform we look over at the other skyscrapers, units with units, vast machines for translating human activity into 0s and 1s, then back again. Extraordinary conceptualism, when one steps outside to contemplate.

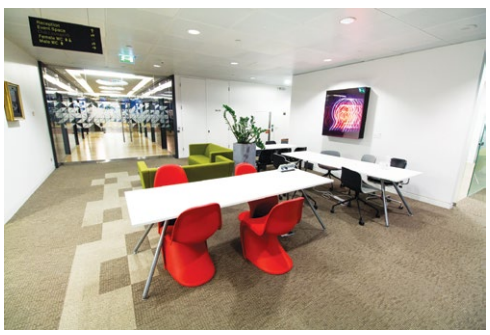
In our role as journalists we find ourselves in many a co working environment, from the subterranean level of London Campus in Shoreditch, known as google campus to everyone in the scene, to Central Working next door, to the WeWorks popping up like so many hives. Each of these spaces have a different feel, a different vibe, reflective of their members.

Google campus is a chaotic cauldron, a reaction vessel, you can walk in with an idea and walk out with a team. But you'll never scale in such a place, too volatile, too distracted, too much. Central Working spaces, each one a different energy, from calm to creative, more like an art school, here's the painters, the sculptors are in another space, each to their own.

Level39 feels... strategic. Poised. Enabled. Serious.
For the space reflects the people, and the people are the companies, 1600 apply, 194 are here. Fintech is finance as technology.

And here, in the calm, above the city, much change is afoot.





LEVEL39

Startups

YIELDERS

What it is: A very interesting company that's what. It's an equity property crowdfunding platform.

How does it work? Properties are placed on the platform. These aren't 'opportunities' or speculative high risk crowdfunding startups. These are bricks and mortar properties that already exist and crucially, are already generating, or contracted to generate, rental income.

Each property has its own SPV. That's a Special Purpose Vehicle. Which is in practice a Limited Company. And it's the shares in theses limited company SPV's that investors buy. They then own a percentage of that property, as an equity shareholding in it, and receive a share of the rental income accordingly.

The tech is not necessarily groundbreaking, but what is very interesting about this business model is the structure of the investment. It's designed to be end to end transacted across the platform, from investing in the property, through to contractual completion, shareholders agreements, shareholders voting, and so on. The platform is the process entire. The implications of this are profound, it simplifies what would be otherwise prohibitively complicated, and in doing so, opens up a new type of investment to the mass market.

From an investment perspective, on the up side there's the appreciation of the property, and the revenue from the rental. The risk side is the property might depreciate, which is possible, but in any event, the rental is fixed, and there's no 'mortgage' to pay. The rental agreements are with housing associations, which means tier one level reliability, with a probably achievable target of zero voids, ie un-rented down time. The rental returns are anticipated to be around 6%.

Another interesting fact about Yielders is that it's based on Islamic banking principles, it's Sharia compliant, which means it's not based on interest charged for lending money.

It's a financial return for a commercial service, in this instance, rented housing.

However, it's not an Islamic opportunity, it's open to anyone with £5000 or more to invest, an amount they plan to lower to £1000 in time. These Islamic banking practices are interesting. It opens up a whole new way of looking at investment, some models of which will be more efficient, better returning, than conventional interest based ones. Forget the religious consideration, from a purely commercial perspective, there's opportunity here, a whole range of investment products are waiting to be interpreted into digitised platforms.

Irfan and Zeeshan are well aware of this. The Yielders platform, with a little white label re branding, could be used to crowd invest in all manner of sectors. Wine. Vintage cars. Art. It's all about the end to end integration of the mechanics of the process, the digital paperwork. Compliance. Definitely one to watch. But then in Level39, aren't they all.

REVOLUTE

What it is:

Physically, it's a card, a Mastercard. With a corresponding app. When activated it becomes a local bank card, where ever you are. You can use it to withdraw funds from ATMs and to buy from shops, and online retailers. In 'any' country.

How does it work?

You open an account in the app. You can then charge the card via the app. You then treat it like a debit card. Which it is. You can have multiple accounts within your account. A dollar account, a euro account, up to 90 currencies.

What's the user benefit?

Convenience, security, and importantly, fractionally the price for overseas use. Users send, spend, and transfer at the interbank rate. Currently 23 currencies to send in.

Founders:

Single founders are the exception to the rule in startups. There are almost no successful ones at all, anywhere. Paul Graham, the mastermind behind Y Combinator, considers single founders to be basically un investable. But there's exceptions to every rule.

Nikolay may be one. With a background in trading, not even in payments, in June 2014, he hired a consultant, one of the top ten in the World apparently, to work out the solution that would become Revolute. The consultant said it wasn't possible, and for that reason wouldn't charge for his expertise, and visited Nikolay in Level39 to explain the process, initially for a day, which became several weeks, as between his experience and Nikolay's, a solution that 'might work' came out of the process.

Sufficiently convinced were Balderton Capital, they seeded it with £3.5M. Investable then. There's now 15 employees, including Veronique, employee number 4, another ex-banking professional, she met Revolute at a meetup, pitched for a job, took it.

I asked Nikolay how much he himself put into the company to get it to that stage. £300,000. It's a different game these ex-banking founders are playing. They themselves are capable of funding their own businesses way above SEIS level angel rounds. I asked the current value of Revolute. Around £26M.

How does it make money? "Not from the users. It's from the shops, a merchant charge, same as shops always pay every time they accept a debit or credit card. Not close to break even yet. Our plan it to make it free forever but to find other sources of revenue, change bitcoins, buy travel insurance, hybrid services, end to end solutions. A Global Money app that allows you to do everything with your money."

I'll say one last thing about Revolute. They know to make things beautiful. Nikolay gave us one of the cards. The mechanism by which you slide open the holder is so satisfying, I must have done it a dozen times, for the pleasure, before even removing the card from the wallet. It's like the elegance of a new iPhone box. It demonstrates an understanding that user satisfaction is not a neutral state, it's a positive one. And the design mind to see it applied, end to end. Revolute. They re-engineer an entire banking process, and I'm still enamoured with the packaging of the card.

BLOCKCHAIN
Diamonds

Chain of disruption

Blockchain wins the war for clean diamonds

While the new kid on the financial technology block, bitcoin, is having a tough time gaining acceptance on the financial playground, its underlying technology, blockchain, is not. Blockchain has been the star attraction at the recent Money 20/20 event in Las Vegas and continues to demand the attention of those who influence both international business and governments.

In an interview for The Fintech Disruptors' Report, Everledger CEO Leanne Kemp talks about the blockchain potential and how Everledger is using the technology to thwart diamond thieves.

"The blockchain represents an opportunity to re-think legacy systems that for the most part have been taken for granted as the way things must be done, rather than what could be done," explains Leanne. "Arguably, the future potential is limitless, particularly in the areas we are focusing on at Everledger: using a global, distributed ledger that cannot be tampered with as a compliment to traditional methods of recording information, all of which have been shown to be vulnerable."

Digital contracts, says Leanne, is one example where transactions passing through multiple intermediaries and countries today are adding unnecessary time and cost to the process. Through the blockchain, it is designed to be self-executing and self-enforcing because the interaction is solely between the parties involved.

Another example involves diamonds. Although many diamond-fuelled wars have ended in Africa, conflict diamonds remain a serious problem. Everledger supports a system of warranties that enable mining companies to verify that their rough stones are not conflict diamonds and comply with the 'Kimberley Process'. The provenance (ownership history) of these diamonds from legitimate sources can be easily accessed by governments, jewellery retailers and consumers, providing full transparency, instant verification of the value and authenticity of the diamonds.

In the six months since its inception, Everledger has already stored the records of over 850,000 diamonds and has impressed its peers by winning the Meffys Award for Fintech Innovation organised by the Mobile Ecosystem Forum – the first blockchain company to be chosen.

For Leanne this is just the start for the technology. "As with others breakthroughs that affect regulations, business systems and human behaviour, adoption will take time," she says. "We're seeing global leaders in technology, like IBM and MIT, turn their focus to developing platform initiatives – even as an open source environment. In finance, 25 banks are now part of the R3 blockchain consortium working to determine a framework for using blockchain technology in markets."

She concludes: "This is progress, but there are challenges such as the legacy of 'bitcoin anxiety' and the need to increase the number of non-tech people who understand and embrace its potential for their business."

RarePink.

New technology meets jewellery

As an online company, trust and transparency is critical to building a respected brand. We are fortunate enough to work with customers at a time where a simple question translates into a life long commitment and promise. As most of our items are bespoke engagement rings, our customers really care that their ring design is one-of-a-kind and that it will remain this way. It becomes a part of the unique bond which has formed, somewhat of an emotional fabric of the relationship. It is for this reason we assure them that each design is made from the mapping of their thoughts and ideas into a truly unique piece. Just as the promise is a one in a life time, so too is their ring and so too is the commitment from Rare Pink.

With emerging technology surging through industry, Rare Pink is at the forefront of embracing these platforms to enable a better customer experience and to protect the promise for the customer. Our existing ethical policy already uses the Kimberley Process, and while this process has proven to drastically reduce the occurrence of conflict diamonds, its paper-based approach is not as rigorous as that of the technology underpinning Everledger when you consider the power of smart contracts and the blockchain.

We hope to be able to proudly say that our ethical sourcing and unique design policies are promises that we can now proudly back-up with technologies that are of the highest security and transparency.

Whilst the diamond industry has been focused on ethical sourcing, the success of these efforts are often blind to the consumer. Enabling the blockchain, and exploring the use of Everledger, enabled another level of transparency to our ethical sourcing policy. Moving beyond the source of the stone, and now we can also protect the designs of our customers and give them a view into this protection through the digital vault technology

A massive additional benefit to our customers is that their design is also protected and thus available for future use should their first ring be lost, stolen or damaged. We look forward to assist out customers in getting their ring insured and increasing the speed through which we can re-make it should we need to where the customer trusts Rare Pink to deliver again on its promise.

BLOGS

16.11.2015
ukbondnetwork.com

Being disrupted isn't just a challenge for the banks

David von Dadelszen
UK Bond Network

In the ever-evolving world of finance, disruption is a challenge for fintech itself.

Financial Technology is a big, growing sector. At the end of last year, Ernst & Young estimated the UK Fintech market to be worth £20 billion in annual revenue, with 18% of this revenue coming from 'emergent' fintech. Whilst financial technology seems to often be perceived as a new phenomenon it seems that, in reality, it is simply a continuation of the natural evolution of the financial services sector.

Financial technology – the use of software to deliver financial services – is continuing to evolve as rapidly as the technology we possess is. Indeed, new technologies are consistently being developed to improve on traditional delivery mechanisms.

Nothing in this world is static. We are in a constant state of flux. Stock exchanges, with their origins in City of London coffee houses at the start of the 17th century, are now almost wholly digital. Complex investment and trading strategies can be deployed at the click of mouse, and we can build equity portfolios with commissions lower than £10 per trade.

One of the most recent, and most talked about developments in financial technology, Peer-to-Peer Lending, now often referred to under the moniker of Marketplace Lending, is gaining huge traction. Whilst the sector seems that it is now undeniably here to stay, it is not without its threats.

The uptake of incumbents

One of the major threats facing the industry is the switching on of incumbent financial organisations to the opportunities presented by leveraging technology to deliver services. The Santander 'InnoVentures' scheme provides funding to fintech startups in exchange for the 'disruptive' technology needed to streamline bank processes and ensure its continued relevance.

Goldman Sachs is actively hiring from the fintech sector, and is planning to launch its own online lending platform in 2016. Hargreaves Lansdown, the UK online financial behemoth, has similar plans in the UK. How the pure marketplace platforms will be affected is yet to be seen. The best outcome is likely to be a significant additional challenge for upstarts to overcome, with a reduced potential ultimate market share.

It is the capital that the incumbents have to deploy that makes them such a threat. Yes, they are being stretched by capital adequacy requirements, but directing a fraction of their turnover to developing digital arms is still entirely possible if the desire to do so is there. If what we are experiencing is however a natural evolution of financial services, the question is, with all the resources available to them, how did the incumbents even let the alternative finance market develop?

Intrinsic challenges

Many leaders of alternative finance platforms used to work in traditional FS organisations, or otherwise larger companies. So the knowledge, and desire, to develop these technologies was there – it just wasn't on the radar of the people at the top.

Leaders of large organisations face an intrinsic challenge when it comes to developing their business. Few are visionaries, instead having proven themselves within the company's existing business model, and excelling at it. Because of this they are experts at what they do, but aren't necessarily naturally inclined to start doing what they do differently.

Embracing change

Flux doesn't just come in the form of the technology that we use; it comes in the form of management styles and organisational culture too. Leaders run the risk of becoming legacy systems themselves – like the technological infrastructure widely noted as hampering change in the banks. Listening to voices from across the organisation – which might be the most junior employees – to nurture both talent and new ideas is incredibly important. What if once a quarter, the CEO sat down with the brightest young talent from each division of its organisation to discuss their ideas? What if when they heard a good idea, they let them run with it within that organisation, giving them ownership (both in terms of an equity share of the siloed business, and in terms of direct management) and let them leverage the organisation's existing expertise to deliver their vision?

Shareholders would need to agree to giving aware a share of new ideas to the individual who came up with the idea and the individual who came up with the idea would need to accept having a lesser stake than if they started the company themselves. But consequently shareholders would own a share of something, which they wouldn't otherwise, and the individual would be able to quickly scale and develop their idea.

While this approach would contribute to an on-going culture of innovation within a business, it would also help to manage the risk of new ideas, which have the potential to take market share away from the business in future. At some point, as the financial services sector continues its ever-evolving cycle we, as disruptive businesses, will ultimately be disrupted too. If, however, we can foster this disruption within our own organisations, put greed to one side and give fair ownership to the owners of disruptive ideas then perhaps we can continue to be the drivers of change in this world, rather than falling prey to ourselves.

BIG PICTURE
Azimo

This changes everything

All big ideas come from either big problems or big opportunities, or at best, a response to both. In the simplest terms, Azimo is a platform to send money online from one place to another. Money transfer. Specifically catering for the market sector of migrant workers. As a company, and a sector, it's literally World changing.

Name: Marta Krupinska

Occupation:
General Manager and Co-founder, Azimo

Born: Krakow, Poland

Education: Masters in Organisational Psychology from Jagiellonian University in Poland and a Management degree from Columbia Business School.

CAREER

2008 – 2011
MD & Founder, Travelnity.com

2012
Somerset House and London 2012 Olympics

2012 – Present
General Manager and Co-founder, Azimo

FAVORITE

Books: Lean In by Sheryl Sandberg
Films: "There Will be Blood" a great example of the emotional price of success

Restaurant: Anything Thai

Hobbies: Travelling and listening to Jazz music

Politics: John Oliver for Prime Minister!

Business philosophy: Success doesn't come from playing it safe. You'll either achieve something great or make a mistake. Mistakes can be key to success, as long as you're ready to act fast on them, learn and next time do better.

Marta gives me the stats: There are almost 250 million migrants, living in 'foreign' countries, and from these, $600 billion is transmitted annually in remittances. A total of 700million people globally send or receive money from abroad.

She quotes Bill Gates who in 2011 said, "If remittance costs were halved from the current average of 10% of the transfer value to 5%, it would unlock $15Billion in poor countries." It's a big 'if', and a big amount of money, Marta puts it in context.

"£15B could feed half of Ethiopia for a year, or provide a mosquito net for every man, woman and child in Africa and Asia." The fee's Azimo charge equate to 2% on average, taking into account the fixed charge per transaction plus the exchange rate.

Even in 2012, Marta explains, people were far from confident in putting their debit cards into a website, and transferring digitally. We have a face to face instinct when it comes to transferring money, it's to do with trust ultimately. We want to see it happen.

Even now, over 90% of remittance happens offline. Branches, shops, tellers, call centers, these all need paying for, ultimately by the customers. I heard a statistic a few days later, from another challenger fintech, they claimed that up to 4% of turnover from some of these companies goes on (non) compliance fines. Again, passed back to the end users in charges and fees. Non digital transfer of money across the World is clumsy, multi processed, risky, and accordingly expensive.

Creating true disruption in any sector frequently comes down to drawing the straightest line between two points. Straightness in process and attitude. This approach, with elegant and robust tech, consistently out competes the 'hidden charges apply' of the past. Azimo is all about transparency and value, disintermediation, removing the middle processes and starting at the consumers' need. It's an ethical quest, moral business, modern business. It's also more effective, more efficient, more straightforward, easier to market. When we step back and consider the norm used to be fundamentally predatory in attitude, it's little wonder times are changing, and difficult to feel any sympathy for the exploitative businesses now trying to hold on to their outdated everything.

"Global poverty could end through the globalisation of remittance ability. Certainly, it can't end without it".

For Marta it's a personal quest, I can feel it and hear it in the language she uses. "...they have the courage to leave their homes, to travel to another country, to work hard and get paid to be able to send enough of that money home to support a family... The most hard working, lowest paid, most exploited... Money transfer isn't a luxury to these 250million people; it's a regular, frequent, necessity."

The modern poor are those who don't have access to remittances. The equalisation of wealth doesn't mean the equalisation of wages. It's the equalisation of access to remittance that's the key to global equality. And the smartphone is the key to all of it.

The number of smartphones is currently on par with the number of bank accounts. By 2020 the ratio will be 3:1. This is going to define the next generation of people, and their understanding of money, what it is, and where it comes from. From airtime credit, digital wallets, to cash from hundreds of thousands of retail points. None of it needing bank accounts.

Global poverty could end through the globalisation of remittance ability. Certainly, it can't end without it.

Smartphones might just be the single most important development in humanitarian terms since... almost anything. The smartphone will enable it, and the money transfer companies, Azimo, Revolut, TransferGo, World Remit and many more, will facilitate it.

It's another level of the Internet of money. The understanding of finance as a technology. And realising its unlimited availability as a consequence.