LEAP 100

City A.M. has teamed up with Mishcon de Reya and other expert partners to identify 100 of the most exciting, fast-growing firms in the UK. They operate at a range of scales and across many sectors, but all are in the process of making the leap to the next level in terms of revenue. We will track the challenges and hopes of this brave and economically vital group, sharing the collective portrait that emerges on this monthly page and at cityam.com/leap-100

On the frontline of the cyber war

Philip Salter speaks to Emily Orton, co-founder of the pioneering cyber firm Darktrace

ON ANY given day, typing the words "cyber attack" into Google News will give you a fresh medley of hacking stories. Hollywood and Edward Snowden may have romanticised the perpetrators of these crimes, but behind most of the headlines sit one or more business owners who are the victims of these devastating breaches.

Darktrace and its 330 odd employees is on the frontline of the fight against the growing menace, employing machine learning techniques based on the biological principles of the human immune system to try to combat cyber threats. Founded three years ago by a group of mathematicians from the University of Cambridge, it is now valued at $500m and backed by former Autonomy entrepreneur Mike Lynch.

At a recent Leap 100 breakfast, one of the company's co-founders Emily Orton gave a detailed overview of the threat landscape to a room full of entrepreneurs, in the process scaring the bejesus out of a fair few of them. Orton is responsible for worldwide marketing for Darktrace, having previously worked at Autonomy and Invoke Capital.

According to Orton, "most of us think about big hacks – for example, TalkTalk and Anonymous – but while that gets a lot of the media attention, the direction we are seeing it going in is far more challenging."

"The most concerning threats that we are seeing are not necessarily targeting your data to take it out of the organisation," says Orton. "We are seeing a move to much more subtle, stealthy threats that are much better at blending into the network and noise of your day-to-day business. They might want to get insights that they can then feed back into the market." Darktrace has uncovered some long-term presences that have been hanging around in a company's network for many months.

We are seeing a move to much more subtle, stealthy threats

A growing threat comes from trust attacks, which aim not to take data but undermine the reputation of the company. "Imagine you're a healthcare company with a lot of patient data. The idea that someone could change even subsectors of that data is far more concerning than a bread and butter data breach, because it could destroy the integrity of the data."

Entrepreneurs are also increasingly faced with ransomware attacks, which block access to a computer system until a sum of money is paid. "We had a small charity in California that got hit by a ransomware attack," says Orton. "You might think: why would anyone want to hack a small Catholic charity in Santa Clara? Well, they are a really easy target. People go after the low hanging fruit before they do the more sophisticated stuff."

And then there is the growing exposure through the internet of things. "The fact that we can connect everyday objects to the network is an absolute nightmare for security," explains Orton. Darktrace spotted some abnormal behaviour at an insurance company. "It was an IP address that we didn't recognise and a lot of data was leaving through the device. We investigated and found that the compromise was with the new air conditioning." US retailer Target Corporation was hacked through network credentials stolen via the refrigeration subcontractor. This supply chain risk is something Orton expects will catch the attention of UK and EU regulators – we have already seen New York start to regulate third-party suppliers.

Finally, there is that ever-present insider threat, which isn't always malicious. "We were working with a games company in the UK", says Orton. Their intellectual property is very important to them because they have groups in China ripping off their games. The company launched a new game but there was a localised version within two days – something that would have taken developers at least six months to copy. "We found there was a user who was regularly sending out source code back to his personal email account on Friday," explains Orton. "He loves developing, so he wanted to do it on the weekend with a beer in his hand and the TV on."

You can't talk, write or work around cyber security without appearing pessimistic. Darktrace and the wider industry is growing on the back of real and present dangers, which are forcing governments to act. But Orton is at pains to strike a tone of optimism and is "very encouraged to see the government investing in this area". This isn't something that government can do on its own, though. The private sector is going to have to do much of the heavy lifting.

Entrepreneurs must be nimble in the face of cyber crime

MISHCON COMMENT

Hugo Plowman

CHANCELLOR Philip Hammond announced last week that, over the next five years, the government will invest £1.9bn in trying to tackle cyber attacks. There's an argument that a sizable chunk of this funding should be directed towards stopping the problem at source abroad, but for UK-based entrepreneurs, their fight against cyber crime will necessarily be fought from their workplace.

Most organisations aren't adequately prepared for cyber risks that change daily. Investment in policies, procedures and training is as important as putting in place the right technology to prevent attacks. However, from startups to the FTSE 100 – one size doesn't fit all. Entrepreneurs should start by identifying what assets are most at risk, how they are most likely to be compromised and what the most proportionate solutions are, bearing in mind that cyber security needs to be realistic.

Employees need to download attachments and click on links to do their job. It is no good trying to implement an outright ban on such activities or trying to discourage normal user activity. So, a business may wish to segregate its information, invest in better contracts, train its staff or hire a full-time security manager.

Whether negligent or malicious, cyber breaches often expose more fundamental weaknesses within an organisation. At some point, an employee is bound to leave a laptop on the tube. If a business is mature in its approach to cyber security, that laptop will be registered, encrypted and wiped remotely. A business that is not sophisticated could lose an unencrypted laptop and not know it's missing for a week because the employee will be too fearful to report it.

Too many companies don't have a plan in place for when things go wrong. We saw this with TalkTalk, which was fined a record £400,000 last month and reprimanded by the Information Commissioner for failing to implement the most basic cyber security measures. TalkTalk didn't know what to say to the press, the regulator and customers, which magnified the problem. Response procedures and communications can be considered in advance, so that customers and the reputation of the company are best protected.

Once you've mitigated cyber risks as far as you practically can, businesses should transfer the remaining financial exposure to an insurer, by putting a proper cyber insurance policy in place. It's comparable to dealing with health and safety risks: identify and mitigate risks, but have general liability insurance to pay for losses that do arise.

The cyber insurance industry remains small in Europe because insurable costs are still relatively modest when compared to those in the US. The new EU General Data Protection Regulation – which will come in before Brexit and sees the introduction of mandatory notification requirements with fines calculated at up to 4 per cent of annual worldwide turnover – should change this.

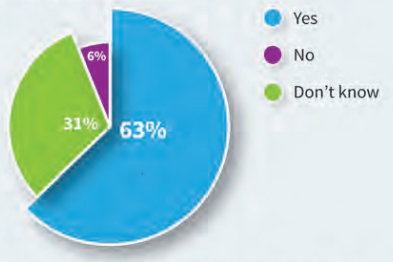
Reacting quickly to a breach can lead to a better result than is often expected – in many cases information and money are recoverable. In a cyber fraud case, criminals can be identified through rapid investigatory work combined with data analytics, and court orders can be used to raid premises to recover what has been stolen and freeze bank accounts.

Entrepreneurs need to be nimble and flexible in the fight against cyber crime. Clearly there are trade-offs when running a profitable business which seizes the digital opportunity, but also seeks to manage cyber like any other business risk. The preparation and fight against cyber threats is a matter of devoting the time and resources to ensure the business is resilient in defence and proactive in attack.

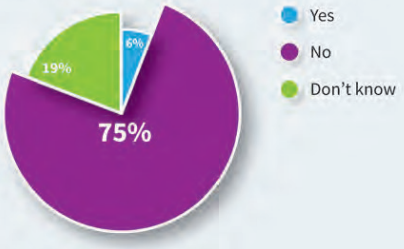
Hugo Plowman is a partner in the litigation department at Mishcon de Reya.

LEAPPOLLING

Do you see cyber crime/cyber attacks as a serious threat to your company?



Have you struggled to employ staff with the right skills to manage cyber risks?



Supporting Britain's scaleups must be a national priority post-Brexit

IF YOU'RE looking for examples of tomorrow's titans, the high-growth superstars that will change our world, you can find an abundance in Britain today.

In fact, 18 of Europe's 47 unicorns – startup companies valued at over $1bn – are from Britain, the highest concentration on the continent. It's a track record that has made the business climate in this country the envy of many parts of the world.

Growth matters. It's how we create wealth, innovate and develop ideas. It's how tomorrow's economy will be built. I remember the former chancellor George Osborne putting the opportunity like this: two thirds of the companies that will make up the S&P 500 in 10 years' time don't yet exist. While his career as chancellor might be over, the prophecy still matters.

Tomorrow's leading firms – the Ubers, Airbnbs and Snapchats – are fixed in the minds of people looking to take the leap today and grow.

Inspired by recent breakout stars, scaleups in the UK are willing to put the bet on themselves and their teams, build businesses that will make a difference and, ultimately, disrupt the status quo.

So far, so good. But since the UK voted to leave the European Union, and the subsequent change of government it brought, my worry is that the laser-sighted focus on the importance of growing firms has been diminished by the elephant in the room. Namely, the long walk to Brexit. And, while trade deals matter, trade matters more.

The conditions that will launch and sustain our future firms are being created today. That's why I have taken the role as

In 2015, tech firms secured almost $1.4bn in funding, 10 times more than in 2010

the chair of the advisory board of The Leap 100 – a grouping of the most exciting, fast-growing companies in Britain. The growth of the scaleup community is something I believe passionately in, not least because, right now, Britain needs a growth project.

In 2011, I was one of a group of co-founders that created the national campaign for startups, StartUp Britain. Back then, Britain needed to focus its energies on creating the climate and culture that could foster startups. Their creation rate was, frankly, falling off a cliff.

I am proud to say that is no longer the case. In fact, in 2015 tech firms secured almost $1.4bn in funding, 10 times more than in 2010.

That next chapter of growth is not just a business priority, it should be the nation's priority. It's why an initiative like The Leap matters.

The leap from startup to scaleup. The opportunity to create world-beaters. A generation of businesses that can make the difference. Businesses fit for the future, able to deliver results today.

Michael Hayman MBE is co-founder of Seven Hills, co-founder of StartUp Britain and co-author of Mission: How The Best In Business Break Through.