MARKET INSIGHT

Insight and analysis from Redmayne Bentley straight to your inbox

Redmayne Bentley

ISSUE 13 - NOVEMBER 2021

Cyber-Wars

IN THIS ISSUE

- Dark Side of the Web
- Cybersecurity: Calculating the Risk
- Lemons, Peaches and Cybersecurity Breaches

CYBER-WARS

JAMES ROWBURY | INVESTMENT RESEARCH LEAD

IN THIS ISSUE

STOCK FOCUS
Dark Side of the Web

READ THE ARTICLE

INSIGHT
Cybersecurity: Calculating the Risk

READ THE ARTICLE

TOPIC OF THE MONTH
Lemons, Peaches, and Security Breaches

READ THE ARTICLE

OPENING HOURS
Monday–Friday, 08:00–17:00

GIVE FEEDBACK
publications@redmayne.co.uk

HEAD OFFICE
0113 243 6941

FOR MORE DETAILS
redmayne.co.uk

FOLLOW US

Our data has become an asset. We use it as currency in exchange for products and services, as internet platforms vie for our attention and collect information on our every move to tailor advertisements and then sell our attention to the highest bidder. When we manage most of our lives online and platforms are making it easier every day to pay for goods or fill out a job application, auto filling and saved credentials are crucial time savers to increase personal productivity. But all this data must be stored somewhere, and someone must protect it.

Cybersecurity is far from a revolutionary industry of this century and one that even predates personal computers (**See: Calculating the Risk**). But in the 1990's, the "PC" became part of the furniture, and anti-virus software was a critical insurance policy to evade the inevitable bugs that would render the family computer inoperable. Thirty years on, PC viruses have seemingly vanished into irrelevance, despite our lives becoming increasingly more connected.

Instead of our own PCs, it is our data that is under attack. This valued asset is becoming a fundamental tool for business, political influence, and even warfare, and thus security is mission critical to companies. As my colleagues write on the next few pages, there have been a multitude of high-profile breaches in the last decade, exposing the vulnerability of firms' poor risk management.

With data becoming ever more sensitive, the cost of these breaches has risen 60% since 2013. Firms are now seeing this as beyond reputationally damaging and instead part of their financial prudence which has seen rise to a multi-billion-dollar market in products and services to protect against these risks. In a survey of business leaders conducted in 2019, cyber incidents topped the list of largest threats to businesses, surpassing both natural catastrophes and new technologies.

So who is going to arm the companies who hold his data? Entering the the UK's markets with a bang, Darktrace is a cybersecurity software company which started as a conception in the minds of Cambridge mathematicians. With such intellectual beginnings, one could assume it is a competent solution (**See: Dark Side of the Web**). Customers clearly think so, with double digit sales growth in its aptly named 'immune system'. Though, investors are more cautious; the firm has demonstrated little appetite to invest in research and development, which is crucial when the enemy is finding new ways to break your defences.

Of course, the challenges posed by cybersecurity present great opportunity. No surprise then that the industry has seen a number new entrants that have crowded the market with supposed solutions to the challenges facing business and governments. Though the complex nature of cybersecurity means searching for the right solution and monitoring its performance is near impossible (**See: Lemons, Peaches and Security Breaches**). Seemingly, the only answer is for firms to overspend and layer solutions over one another in the hope that one will provide a line of defence in the event of an attack.

STOCK FOCUS

DARK SIDE OF THE WEB

It is fair to say the UK stock market has not been blessed with the high-growth, technology focused businesses that have become the centrepiece of the US market over the past decade. Instead, it has become commonplace for the UK market to be associated with slower growth, more traditional businesses that focus on exercising prudence ahead of any blue-sky aspirations. However, it appears that the FTSE 100 is now home to one of the world's fastest-growing cybersecurity companies.

Founded and headquartered in Cambridge, Darktrace (DARK) was set up in 2013 by a group of mathematicians and cyber defence experts and has quickly grown to become one of the hottest names in cybersecurity. The technology itself champions a new category of cyber solutions based on Bayesian mathematics developed at the University of Cambridge.

The business' core platform is named "The Darktrace Immune System" and, like any functioning immune system, the platform will detect and neutralise foreign threats before using data from the attack to build defences that prevent any same breach from occurring twice. This is achieved via one of the first at-scale deployments of machine learning and artificial intelligence (AI) within a cybersecurity product. The immune system embeds itself within the customer's operational systems, continually learning and evolving alongside the business to provide security, but also will likely deliver significant cost savings over time.

As the digitalisation of business and the economy continues to increase it is no surprise that the cybersecurity market is forecasted to grow rapidly in size. Short-term forecasts predict that the cybersecurity market will be worth over double what is today by 2026, growing to a total market value of US$398.3bn. However, perhaps a more important measure when assessing the value of such security systems is the potential cost of cybercrime to businesses and the global economy which analysts believe will hit US$10.5tn by 2025.

Despite this clear market opportunity and the potentially ground-breaking nature of Darktrace's offering, the stock itself hasn't been without controversy and, with that, volatility. Firstly, prior to the initial public offering (IPO) in April of this year the valuation was cut due to links to alleged fraudster and former Autonomy CEO Mike Lynch, who had been an early supporter of the business via his venture capital fund, Invoke Capital. While this may have spooked investment banks supporting the issue, the shares surged 43% from the issue price of £2.50 on the first day of trading. The shares then rallied further from this point touching £9.85 in late September when the business blew away previous expectations to deliver annual revenue growth of 41.3%, alongside 45.3% growth in new customers.

Such strength continued into late October before the tide turned when questions were raised against the nature of the business' product and their ability to compete with competitors who boasted larger research and development (R&D) budgets. On the first point, it was suggested that the highly involved nature of the immune system product increased the complexity of integration and wouldn't be suitable for all businesses, thus reducing the size of the target addressable market. On the second point, fears were raised against the ability of the business to defend its strong market position as larger, well-capitalised competitors begin to enter, who could effectively dwarf Darktrace's R&D budget which, may result in Darktrace's offering quickly becoming outdated.

Given that the strong run since April had effectively led the shares to be priced for perfection, these fears created significant volatility with the shares shedding 20% of their value within a day. Such sentiment was then compounded as the 180-day investor lock-up period for those invested pre-IPO ended. As a result of the end of this lock-up period, Vitruvian Partners sold £63.8m worth of shares at an 8% discount to the market price. The sale accounted for approximately a third of their total stake and raised fears that more could follow suit. Shares appear to have settled down following the October chaos, but remain 38% below previous highs, so the question for investors becomes whether the recent pullback was based on fact or fear?

The market opportunity for a company such as Darktrace is undeniable, and the product has gained credibility via collaborations with Amazon Web Solutions (AWS) which awarded the business two accreditations relating to the performance of infrastructure. Beyond this, the customer base has now grown to service over 5,500 businesses from a highly diversified range of industries demonstrating the wide-reaching application of the technology. However, given the rapidly changing nature of the sector as cybercriminals employ increasingly sophisticated methods of deception, a business's ability to replenish its technology via R&D will be key to maintaining a competitive advantage and thus is a factor that will need to be closely monitored as well capitalised players enter the market (**See: Lemons, Peaches and Security Breaches**). In addition, despite strong growth trends the business is still yet to turn a profit which will likely create future volatility due to valuation concerns.

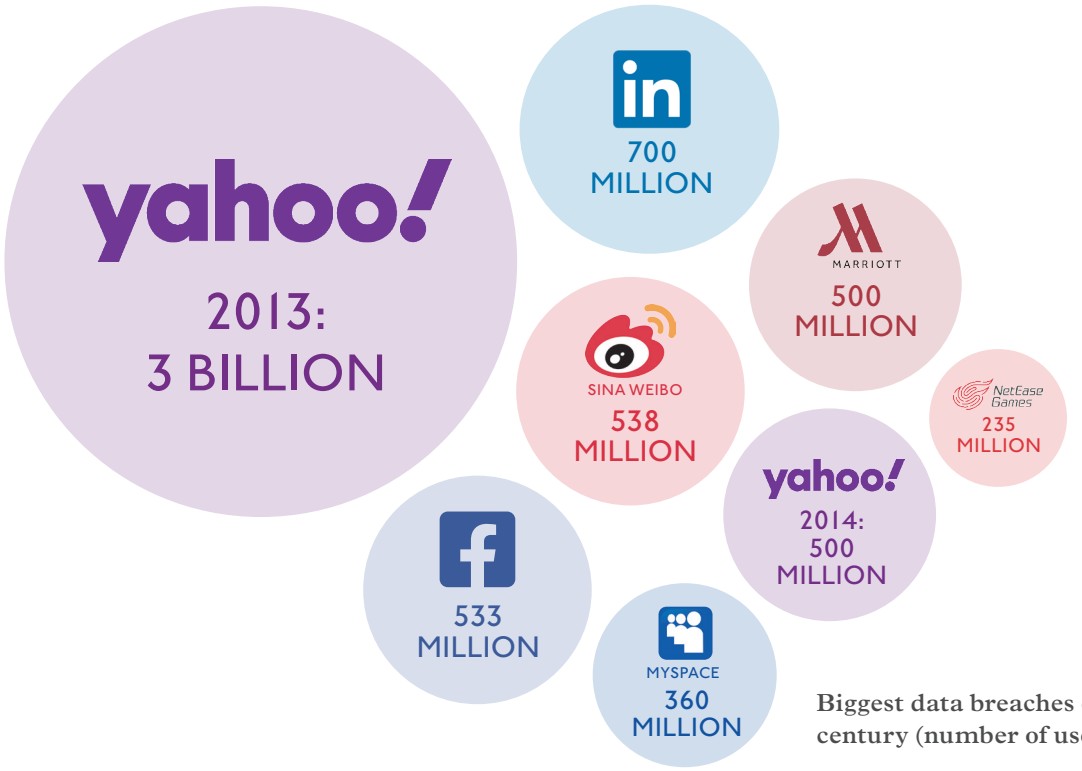
"The market opportunity for a company such as Darktrace is undeniable, and the product has gained credibility via collaborations with Amazon Web Solutions (AWS) which awarded the business two accreditations relating to the performance of infrastructure."

As is often common it is likely the truth lies somewhere in the middle, it is fair to say the exponential growth witnessed since the IPO led shares to get a little bit ahead of fundamentals and thus a pullback down to reality was likely due. With that being said, it is not often that the UK market provides an opportunity to invest in a technologically advanced business well-positioned to serve a structurally growing market and thus to bet against the businesses success over the long term could prove foolish. ■

Please note that this communication is for information only and does not constitute a recommendation to buy or sell the shares of the investments mentioned.

INSIGHT

CYBERSECURITY: CALCULATING THE RISK



Biggest data breaches of the 21st century (number of users).

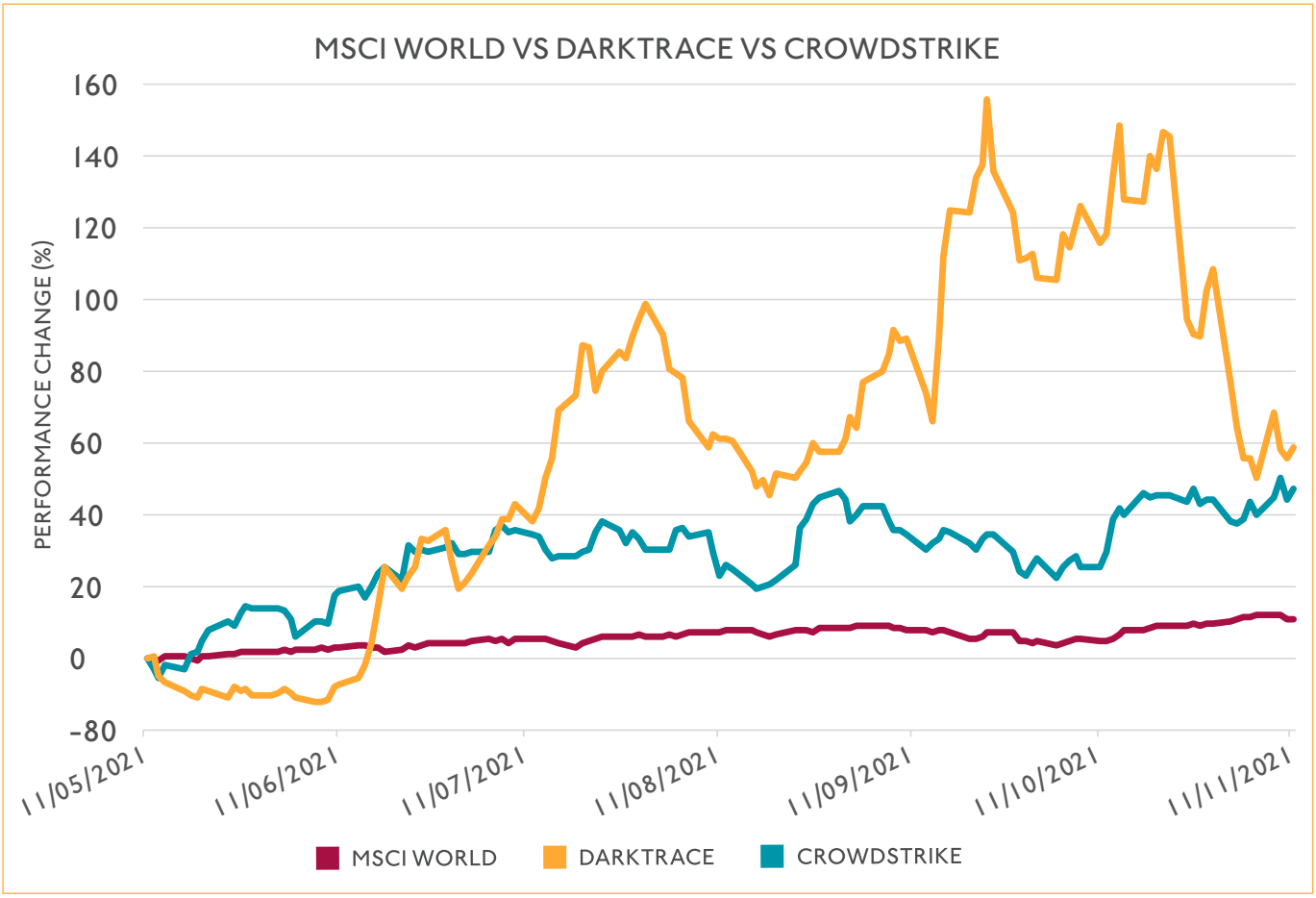
Source: www.csoonline.com

The birth of the internet has given rise to a new breed of criminals, one that does not have to rob a physical bank or person. In fact, much of their work can be done from the comfort of their own home, 24 hours a day, seven days a week. Cybercrime has ballooned into a £27bn per year problem in the UK, fuelling demand for cybersecurity products as a way to protect intellectual property (IP), trade secrets and, of course, money.

The first ever 'hack' was carried out in the 1960's by students at Massachusetts Institute of Technology (MIT) who attempted to improve and test the limits of model trains. They eventually moved on to computers, attempting to improve their efficiency, however, these days hacks are often seen as more malicious attacks on data and sensitive information. By the 1990's the world had started to adopt the computer as standard and virus and malware numbers had already started to increase exponentially.

Skip forward to 2021 and cyber-attacks have become ever more prevalent and costly to organisations and individuals. The dangers of attacks on sensitive personal information are clear and the list of options available to criminals once this data has been obtained is lengthy. Identity theft, such as using victims' credit cards, and using sensitive information to harm organisations, are both examples of how personal information can be used by hackers to eventually obtain money. As such, this data is extremely important.

While there have been numerous larger attacks, the 2017 Equifax and 2014 JP Morgan data breaches show the highly sensitive nature of data that can be stolen. Bank details and credit history can be used in a number of ways, leaving fraudulent loans taken out in people's names or cash simply taken from their bank account. Such financial institutions are entrusted with client information, as well as money and investments, and with millions of US, UK and Canadian



Source: FactSet

citizens effected by both attacks, it calls into question the effectiveness of such firms' cyber protection, especially given the nature of the data they hold.

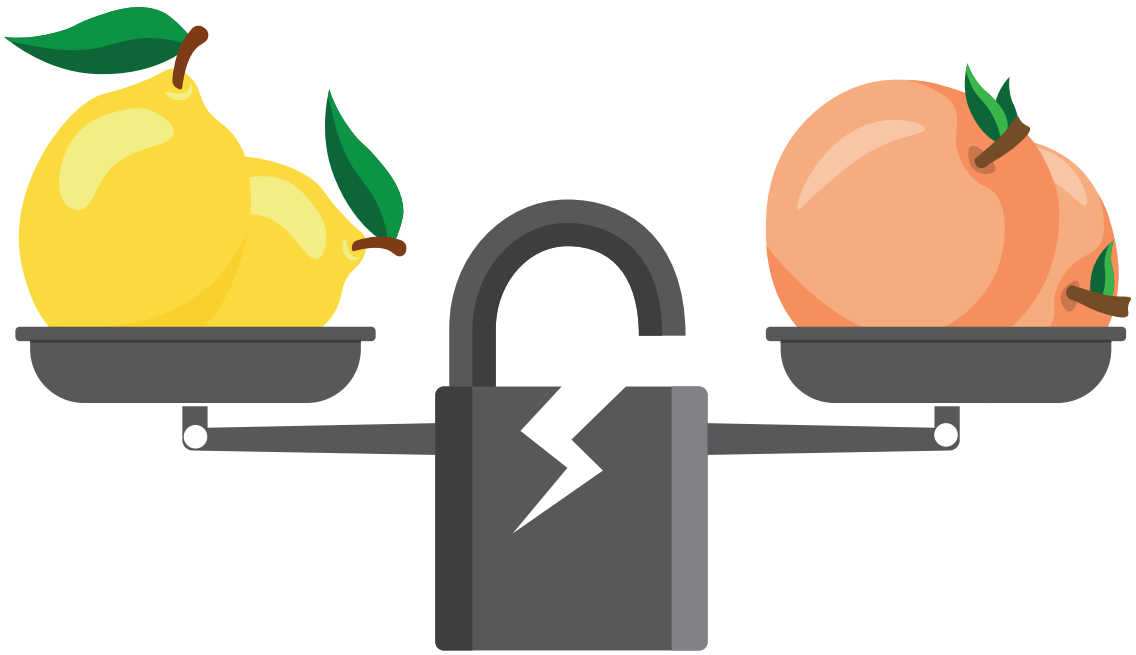
However, nowadays there are several reasons for companies to take their data security seriously, not least due to the reputational and financial risk, but also the increasing regulatory scrutiny and penalties that can come with it. Under GDPR rules, breaches can be met with fines of up to €20m or up to 4% of a company's global turnover, whichever is higher. Such incentives to protect from the severe risks involved have helped to foster new age cybersecurity companies that utilise the most advanced technology in order to protect their client's data. Firms such as Darktrace and Crowdstrike have created and nurtured extremely complicated and advanced products that use artificial intelligence and machine learning to both learn from previous attacks, as well as predict future ones, helping to build a broad-based and highly effective defence against cyber-attacks. Typical legacy cybersecurity providers have long since lacked the investment into research and development (R&D), developing products that are typically easily sidestepped by hackers and sold on a one-off basis, meaning that their customers are faced with large invoices from the start.

The new, high-tech firms, however, typically sell their products on a subscription basis, meaning that businesses have low, regular monthly payments and any upgrades to the products are often included in the price with perhaps small, occasional uplifts in cost each year. This has meant that such firms, which are often small or medium-sized businesses, have been excellent investments, typically right from the point at which they listed on the stock market. Since its initial public offering (IPO) in April of this year, UK-based Darktrace has outperformed the CBOE UK All Companies index by over 77% and Crowdstrike, a US-based competitor, has risen an astronomical 347% since its IPO in June 2019. These instances of incredible share price growth are not without merit. Both companies have been working hard on pushing the advantages of their products, spending heavily on R&D and sales and marketing, subsequently growing revenues exponentially by taking market share from the legacy incumbents.

We would expect this trend to continue as such companies continue to embrace technologies that are able to constantly improve their product and ensure their customers remain protected from malicious cyber-attacks. The industry itself offers a wide array of attractive demand tailwinds from corporate risk mitigation to legal adherence and this should see it grow at a consistent and healthy rate for some time to come. With fast-growing, new-age technology companies the norm, the sector remains a stock picker's paradise, with those companies carving out market share likely to remain very strong investments for some time. ■

TOPIC OF THE MONTH

LEMONS, PEACHES, AND SECURITY BREACHES



In his seminal 1970 paper, Nobel Prize-winning economist George Akerlof demonstrated the tendency of markets to break down in the presence of asymmetric information, applying it to the used car market. While salesmen knew the quality and true value of the car they were selling, consumers were unable to tell the 'lemons' (shoddy cars) from the 'peaches' (quality cars). This uncertainty made consumers unwilling to pay for peaches, in case they were lemons, and made them overpay for lemons, in case they were peaches, incentivising the provision of lemons. This analysis can be applied to the complex and mystifying world of cybersecurity.

Cybersecurity budgets are soaring, rising nearly 60% between 2014 and 2019 – the number of security breaches rose nearly 70% in the same period – and by nearly another third since. Despite this, standards are failing to keep pace, suggesting that more investment is required, with a study revealing that 90% of over one hundred experts in the field believe cybersecurity is not good enough. When assessing the efficacy of cybersecurity solutions there are four broad measures: how capable the product is to perform its function, how well it works in reality, how well it was built, and the security of the supplier.

PRODUCT COMPLEXITY

To the untrained eye, complexity is impressive; to the trained, the opposite is true. Many products are overcomplex; the more overcomplex the product, the more likely it has undetected design weaknesses and the more likely it is insecure. Since firms are wary of their security systems failing, they layer solutions on top of each other, which is cost-inefficient and leads to overspending. This increases complexity in already complex systems and, by extension, the workload on each system which must interact with and monitor the other systems, reducing their efficacy. Overworked systems then process complex data, which is more likely to cause a false positive and then be analysed, raising the chances of data slipping through. An important point to note is that complexity increases opacity. It becomes difficult for a firm to assess or audit its own security systems and cybersecurity firms rarely share the limits or true efficacy of their products.

RISK AVERSION

Partly due to the lack of available information, the industry is awash with risk aversion. Cybersecurity tools need to be executed perfectly and even standard firewalls are hard to set up. As a result, when chief information security officers (CISOs) inherit legacy systems and do not understand their efficacy or workings, they keep them for fear of what could happen if they changed it. Often, intermediaries are used to advise on the sea of solutions available, and are themselves risk averse, generally preferring the 'industry standard'. In so doing, they cannot be held accountable when things go wrong, unlike the 'riskier' new option, and stifle innovation while entrenching broken norms.

RUTHLESS COMPETITION

An inability to differentiate between good solutions and bad means that success is a matter of marketing, not of quality products. This creates a feedback loop where many companies exist in cutthroat competition, spending extravagantly on marketing to tread water rather than investment, which prevents a quality product from being either created or marketed competitively, ultimately maintaining the cutthroat competition. The high levels of competition mean new products are typically brought to market only 60-70% complete, and low-level developers under pressure cut corners and exaggerate their products' capabilities.

ASSESSING THE CROWD

If the market is rife with incomplete, flawed products, and the intermediaries offer inadequate answers, the onus is on firms to make the right choice. Free risk assessments are the common measurement of efficacy, but usually only assess the solutions with checklists. Selected labs, for a fee, offer varying levels of risk assessment including penetration testing (full scale hacking operations on security systems) and risk assessments that prioritise risks. One such lab, ScienceSoft, uses techniques from sophisticated web-based hacking to social engineering to identify employee vulnerabilities. This and softer services provide firms with detailed reports and actionable recommendations. When data and information are so valuable, it makes sense for firms to take their time to validate the claims of new providers and test the defences of existing system's software updates.

"A firm that subjects itself to rigorous, well-funded and independent testing regularly in the interest of its customers is not only a sign of a good product, but a great sustainable culture."

A GAME OF RESOURCES

A self-explanatory solution is to allocate resources to the problem; an illustrative example reveals its root. Product A, for example, has £300,000 spent on penetration testing, but is tested by 30 different clients with a budget of £10,000 each. This means a hacking group only needs a budget of more than £10,000 to find flaws the tests otherwise missed, and they often have considerably more. This could call for groups of clients respective to a product to pool penetration testing resources and force improvements, though it would be difficult to execute. The more that is spent on testing, the more the best products will come to the fore in the long run.

LESSONS FOR INVESTORS

What lessons can be drawn from this? In selecting cybersecurity companies, many embrace those that innovate away from industry norms. They look for simplified, differentiated products that are made easy to understand (if you can understand the solution then so can customers), and longer development cycles that indicate a more complete product. A firm that subjects itself to rigorous, well-funded and independent testing regularly in the interest of its customers is not only a sign of a good product, but a great sustainable culture. ■

Redmayne
Bentley

redmayne.co.uk