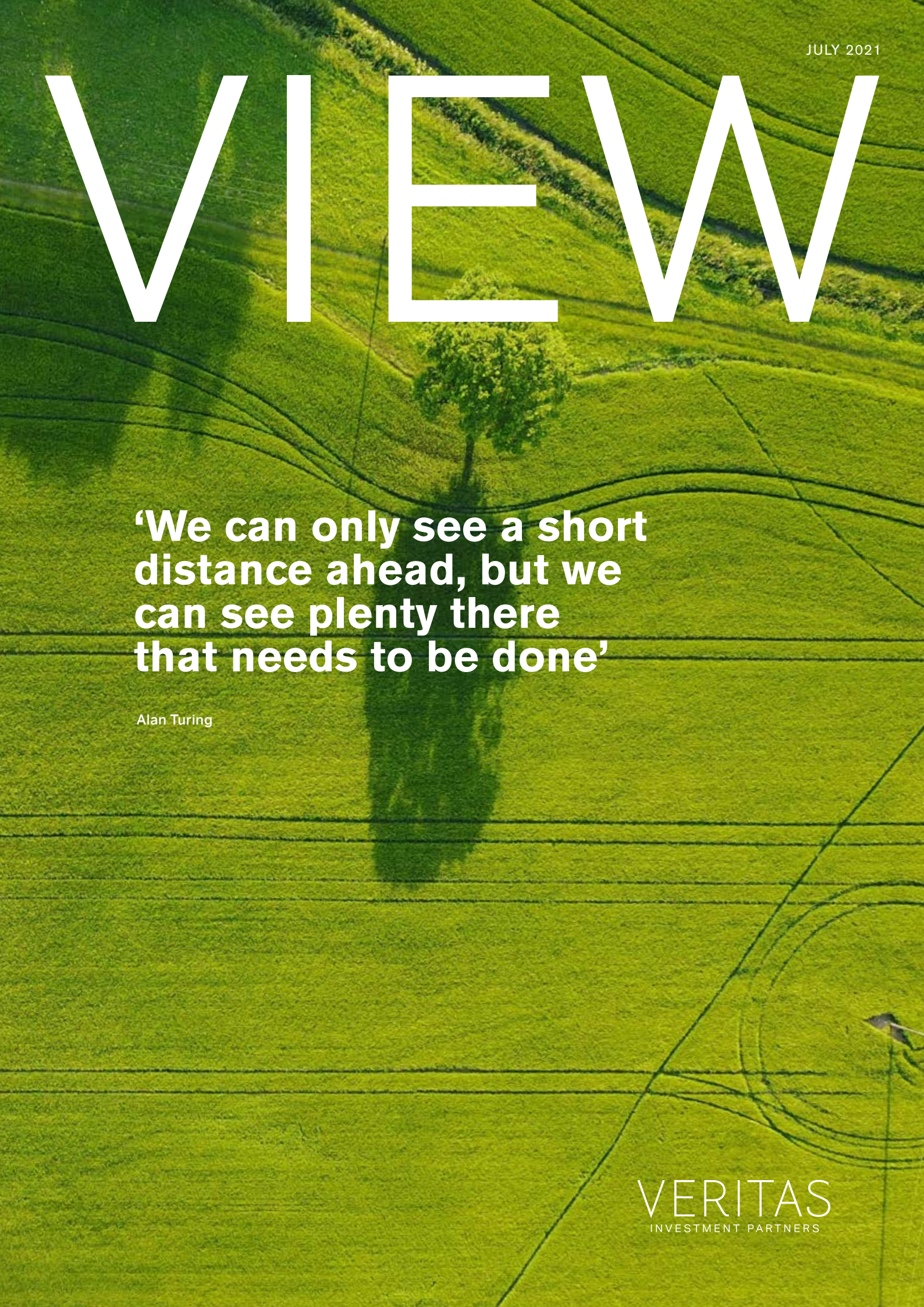
JULY 2021

VIEW



‘We can only see a short distance ahead, but we can see plenty there that needs to be done’

Alan Turing

VERITAS
INVESTMENT PARTNERS

WHEN DISASTER STRIKES, THE TIME TO PREPARE HAS PASSED

On what would have been his 109th birthday, a new £50 note was launched to commemorate the legacy of Alan Turing this month. As one of the earliest pioneers of artificial intelligence (AI), he probably would not be shocked to know that the global AI market is now valued at over $325 billion[1] and is being used for good around the world, from advancing cancer treatments to exposing human trafficking networks[2].

But where there is light, there is also darkness. AI has become a tool-of-choice for hackers. Cyber crime has been around for many years: the first ransomware attack was made in 1989 with a virus spread by floppy disks[3]. But the accelerated shift to digital during the lockdowns of the past 15 months has sparked a crime boom. From phishing emails and "smishing" texts (our UK-based readers might have seen messages claiming to be from Royal Mail about fake parcels) to ransomware attacks, incidents are on the rise, and they are becoming more sophisticated. If cyber crime were measured in terms of GDP, then it would be the third-largest economy after USA and China[4]. And it shows no sign of shrinking: by 2025, the cost to the global economy is expected to be $10.5 trillion, almost $20 million every minute[5].

When disaster strikes, the time to prepare has passed[6]

As running a business from an off-grid bunker is clearly not an option for most, this is one of those times when preparation really is imperative, and no organisation is exempt. The Vatican Library is putting AI to good use to protect digital copies of its masterpieces. A collection that includes Michelangelo sketches would be quite a find for a ransomware attacker[7].

Even with the best security, organisations can still fall victim to an attack but with suitable measures in place, they at least stand a chance of minimising significant financial and regulatory damage. Asking investee companies about their approach to understanding, managing and monitoring cyber risks has long been part of our engagement work. In 2017, our meeting with cyber experts Darktrace highlighted that focusing on individual types of cyber defence, like firewalls, will no longer suffice. On today's cyber battlefields, companies need fully integrated protection, including AI to spot and investigate unusual activity before it escalates to a full-scale attack. Therefore, the questions we ask companies aim to understand how cyber security is embedded throughout operations, from front line systems to boardrooms and, where an attack has occurred, what steps have been put in place to prevent another one. All stocks in portfolios have board level or senior management responsibility for cyber security.

At the same time, the market for cyber protection is growing. And just as they are positioned for the shift to the digital world we discussed in our previous note, companies in portfolios are well-placed for it. Consultancy firm **Accenture** offers clients a full suite of solutions to cover the range of threats they face today. It now has revenues of just over $3 billion from cyber security[8], broadly equivalent to the revenues of Palo Alto, one of the leading standalone cyber security companies.

Following the money... and the devices and the data...

Unsurprisingly, banks have been amongst the worst hit organisations providing criminals with the most "buck for their bang". But the rapid rise of connected devices has opened up vast new markets for hackers, turning the Internet of Things into the Internet of Threats. Help is at hand from companies like **Infineon Technologies** whose chips embed security into the hardware of devices to provide a strong foundation for additional security applications.

And as the global repository of data has ballooned, so too has its value to hackers. Over the last year, the healthcare sector has been in the firing line especially as the use of remote services, such as telehealth, has grown. In the US alone, nearly 500 healthcare providers were victims of cyber crime, affecting over 16.5 million patients[9]. Ransomware attacks have hit hospitals around the world, most recently in Ireland.

Healthcare organisations are lucrative targets for hackers. Because of the critical care they provide, having systems out of action is simply not an option.

1. https://www.statista.com/topics/3104/artificial-intelligence-ai-worldwide/
2. https://www.accenture.com/gb-en/services/ai-artificial-intelligence-index
3. The Economist, 25 June 2021
4. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
5. https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/
6. Steven Cyros
7. https://www.theguardian.com/world/2020/nov/08/vatican-enlists-bots-to-protect-library-from-onslaught-of-hackers
8. https://www.accenture.com/gb-en

Plus, they often face the threat of "double extortion" where criminals not only hold systems hostage but also threaten to leak sensitive patient information online. This is something healthcare technology company **Cerner** knows well and its multi-layered approach to security is designed to keep patient records safe and healthcare providers fully operational.

Of course, keeping a business safe from all cyber attacks would be the ideal scenario but increasingly that seems to be a pipedream. This is where insurance against cyber crime can help but estimates suggest the gap between the cost of cyber crime to businesses and the cost of insurance premiums paid is well over $400 billion[10]. To make it easier for customers to access cyber insurance, **Intuit** has a partnership with insurance provider Coalition. Small businesses can now buy insurance directly through Intuit's QuickBooks accounting system[11]. Meanwhile, as a leading broker of cyber insurance, **Marsh McLennan** is using its expertise to help clients navigate a tricky area. For many companies, cyber insurance is completely new territory, and the advice of experienced brokers can be invaluable.

We are the weakest links

While ransomware attacks have hit the headlines recently, individuals falling for phishing emails remains the most common cyber problem, responsible for over 30% of all global cyber attacks[12]. For businesses, combatting this cannot be done by technology alone: it will require investment in people and a culture of openness and continuous learning. This is one reason why questions about culture and training opportunities feature on so many of our agendas for company meetings.

As you would expect when trusted with the data of 1.3 billion people and 166 million businesses globally, **Experian** has state-of-the-art security. But the company goes further, embedding a commitment to "treat data with respect" throughout its strategy and offering over 250 training courses to staff every year to give them the latest information about keeping data safe[13]. Upskilling more broadly is an important weapon in our armoury. Estimates suggest that the world is facing a shortfall of 3.5 million security personnel[14]. Fortunately, innovative approaches to this abound, such as **Mastercard**'s Girls4Tech education programme which features special modules on cyber and cryptography.

Is honesty the best policy?

All of this has created an interesting fusion of business and geopolitics in which interests do not necessarily align. In some countries, it is already illegal to pay ransomware demands and others are considering going down the same route, fearing that a willingness to pay gives hackers greater incentive to attack critical infrastructure. Many security experts would like companies to be open about attacks they have suffered so that knowledge can be shared, and lessons learned. Some governments are considering making this a legal requirement. But for companies suffering an attack, these could be bitter pills to swallow.

Increasingly companies are competing on an uneven playing field and the odds are not in their favour. Security experts believe that the most successful hackers today are either directly backed, or tacitly tolerated, by nation states and have significant resources to devote to their activities. It has also been reported that hackers have begun to steal and hold onto encrypted information with the belief that in the not-too-distant-future, they will have the technology needed to read it thanks to developments in quantum computing.

"We can only see a short distance ahead, but we can see plenty there that needs to be done". Mr Turing was certainly right about that. The past year has demonstrated the importance of preparing for the unexpected. It is impossible to know what cyber threats lie ahead but we do know they will continue to evolve and that we must continue to do what we can to be ready for them. Our commitment to protecting and growing our clients' assets means that cyber security will continue to be a relevant topic for our company engagements. We want to ensure that our companies remain focused on the risks from cyber security while continuing to take part in the search for solutions.


Written by **Philippa Bliss** and **Catriona Hoare**
on behalf of the Investment Team

9. https://www.cerner.com/perspectives/the-4-cybersecurity-resolutions-every-care-provider-should-make-in-2021
10. https://www.aon.com/2021-cyber-security-risk-report/
11. https://www.channele2e.com/business/small/coalition-intuit-cyber-insurance-smbs/
12. https://www.visualcapitalist.com/investing-in-core-cybersecurity-technology/
13. https://www.experianplc.com/responsibility/treating-data-with-respect/
14. https://www.microsoft.com/security/blog/2021/03/02/4-ways-microsoft-is-delivering-security-for-all-in-a-zero-trust-world/

SPOTLIGHT:

WE CANNOT SOLVE OUR PROBLEMS WITH THE SAME THINKING THAT CREATED THEM[15]

Just as we need cutting-edge ideas to fight cyber crime, we need innovation to tackle the environmental and social challenges the world is facing. In a year which includes the UN COP26 Climate Summit and its Biodiversity Convention, debate about how we manage the planet's resources while meeting the needs of a growing population has reached fever pitch. As some of the largest companies in the world, our investee companies have the scale to reach billions of people and the resources to tackle today's problems head on. Providing these solutions can also make business sense too and some examples of this in action are included below.

Unilever – **2.5 billion** people use its products every day. One area where it has the scale to have impact is reducing plastic waste. By 2025, it aims to ensure 100% of plastic packaging will be fully reusable, recyclable or compostable. Examples include Dove's "beauty refill-ution" where deodorant is sold in a refillable stainless-steel case and fully recyclable toothpaste tubes[16].

Microsoft – Its impact is spreading far beyond its own business as it builds the **Planetary Computer** which will combine data, AI and Microsoft's cloud infrastructure to provide access to critical environmental datasets. This is in addition to commitments made for its own business, such as removing from the environment all the carbon it has emitted since it was founded in 1975[17].

Infineon Technologies – Its chips contribute a net ecological benefit through a reduction in carbon emissions of **54 million tonnes** of CO_2 per annum. This is equivalent to emissions generated by the average annual electricity consumption of 90 million people living in Europe[18].

Kuehne + Nagel – It is helping to clean up the shipping industry though its **Net Zero Carbon Programme**. The range of measures in place to help customers meet their own sustainability targets include switching to the biofuel 'Used Cooking Oil Methyl Ester' (UCOME) which neither requires farmland nor interferes with food cultivation[19].

Bunzl – Its sustainable products include the **reusable and compostable bags** provided at several UK supermarkets which are used by thousands of shoppers every day. Own-brand sustainable ranges tend to have higher margins than other products.

Hasbro – All of its toy packaging will be **plastic free** by 2022 and it runs an industry-leading toy recycling scheme around the world.

Thermo Fisher Scientific – Thermo supplies analytical instruments which are used in multiple environmental studies around the world, from **monitoring air quality to identifying microplastics**.

We look forward to sharing details of how our companies are helping to tackle social issues in the next edition of VIEW.

15. Albert Einstein
16. https://www.unilever.com/planet-and-society/waste-free-world/rethinking-plastic-packaging/
17. https://blogs.microsoft.com/blog/2020/01/16/microsoft-will-be-carbon-negative-by-2030/
18. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWyG1q
19. https://home.kuehne-nagel.com/documents/20124/341873/Kuehne-Nagel-Sustainability-Report-2020.pdf/352d134d-9811-2f22-bc19-4c4610b8da0f?t=1621959636908

VERITAS
INVESTMENT PARTNERS

Veritas Investment Partners (UK) Ltd
Riverside House, 2a Southwark Bridge Road,
London, SE1 9HA
T +44 (0) 20 3740 8350

Veritas Investment Management AG
Genferstrasse 21,
8002 Zürich, Switzerland.
T +41 (0) 44 206 2660

If you no longer wish to receive View, please contact us on either of the above numbers.