Annual Report
Darktrace Holdings Limited

For the year ended 30 June 2023

Company No. 08562035

Contents

Company information

Company registration number:	08562035
Registered office:	Maurice Wilkes Building St John's Innovation Park Cowley Road Cambridge CB4 0DS
Directors:	Ms C Graham Mr J Sporle
Auditor:	Grant Thornton UK LLP 30 Finsbury Square Finsbury London EC2A 1AG

Strategic report

Introduction

The Directors present the strategic report of Darktrace Holdings Limited for the year ended 30 June 2023. Darktrace Holdings Limited ('the Company' or 'Darktrace') has a well-defined strategy to leverage its market-leading technology and first mover market position to drive growth by capturing an increasing share of a rapidly expanding market.

Principal activity

Darktrace's proprietary Self-Learning Artificial Intelligence (AI) technology differentiates the Company from others in the cyber security industry. Its success has been built on a determination to approach cyber security through a fundamentally different lens, which thwarts threats already inside an organisation based on its understanding of what 'normal' looks like. Rather than learning from historical data, Darktrace DETECT™, powered by Self-Learning AI, continuously learns how an organisation operates, which enables it to identify deviations from the norm that may signal threats, including the novel, unpredictable attacks that are missed by other defences. Darktrace RESPOND™, our autonomous response technology, acts as a micro-decision-making AI engine, disarming threats like ransomware before they escalate into a crisis. Darktrace Cyber AI Analyst™ takes this a stage further by automatically investigating in the background every security event surfaced by Darktrace DETECT™. Using Explainable AI supported by natural language processing, Cyber AI Analyst™ produces clear reports that help human teams prioritise where they should focus. All of these capabilities support the Cyber AI Loop™, the AI engines creating a feedback system in which each product continuously and autonomously hardens the entire system.

The acquisition of Cybersprint, an attack surface management company last year, enabled the Company to accelerate the launch of the new product family, Darktrace PREVENT™, in July 2022 – the third component of the Cyber AI Loop™ and a significant development for the Company's long-range technology vision. With PREVENT™, the Company can help its customers to proactively spot vulnerabilities before attackers get to them, and subsequently harden the business' defences inside and out to ensure these vulnerabilities are not exploited. PREVENT™ includes two new products – Darktrace PREVENT™/End-to-End™(E2E™) and PREVENT™/Attack Surface Management™ (PREVENT™/ASM™). Based on the understanding of 'self' for a business, these products will allow Darktrace to get into the mindset of an attacker, using AI to analyse the critical pathways within a business, based on its understanding of all the theoretical routes an attacker might take, and then prioritise and wrap protection around the vulnerabilities that matter the most. With PREVENT™, the Company is making the job of a cyber-attacker much harder. In the longer term, management believes these technologies may be applied to adjacent opportunities to support risk reduction, compliance and IT.

Review of trading results

Strong Financial and Operational Performance

Darktrace Holdings Limited financial performance for the year has been robust, delivering on growth and demonstrating the underlying strength of the business model, all whilst continuing to invest in the business. Company adjusted EBITDA increased to $105.0 million, up from $68.1 million in FY 2022, and delivered an operating profit margin of 5.4%. The macro-economic backdrop has been a headwind for many businesses over the past year, and we have not been immune from its impact. Darktrace now has 8,799 customers globally but have seen a slow-down in new customer additions at a rate of 13.8% below the prior year - as pressure on business budgets has meant that prospects have been more reluctant to run product trials. We are continuing to generate cash, which has enabled us to continue investing in our product pipeline and go-to-market operations, positioning us for the next phase of our growth journey.

Continuing to Innovate

Darktrace has a history of innovation. It started with the launch of DETECT in 2013, which enabled human security teams to see any and all threats inside their organisation. A few years later, Darktrace released RESPOND to the market allowing our customers to surgically stop anomalous behaviour while allowing normal business activity to continue. At the beginning of this fiscal year, Darktrace reached another milestone with the launch of PREVENT in July 2022 which proactively hardens defences for our customers based on its unique understanding of their business. Just as the Company entered FY 2024, Darktrace launched HEAL which supports security teams to recover the business back to a healthy state after an attack and enhances the capabilities already provided in PREVENT, DETECT and RESPOND.

All of this is down to the hard work of the technology team, led by the Chief Technology Officer, Jack Stockdale OBE, which has driven forward this ambitious technology vision and achieved what no other cyber security vendor has. The strong team in our Cyber AI Research Centre has continued to innovate on existing capabilities so that every element of the offering to customers is one step ahead of the fast-moving threat landscape and delivering value to customers.

Building and iterating on the product set since Darktrace set out on its mission in 2013 and will continue to do so. Darktrace trained its own large language models on proprietary Darktrace security datasets and released them as part of its product in 2021. Darktrace is already using generative AI in its attack simulation phishing product as part of PREVENT, and in its Cyber AI Analyst to perform incident investigation and analysis. Looking ahead, the technology team is examining how this can power new chat interfaces in Darktrace products, create new and novel versions of simulated table-top exercises in HEAL, and generate, summarise and translate reports across the products. While the rest of the market is racing to keep up, Darktrace is one step ahead - because this era of AI-powered attacks is what Darktrace has been preparing for.

Strengthening our Management Team

Darktrace continued to invest in its people and have been focussed on bringing in experienced top talent to help on the next phase of its growth journey. In July 2022, Carolyn Esser joined from the Bill & Melinda Gates Foundation as Chief Corporate Affairs Officer, and is responsible for Darktrace's internal and external communications strategies, reputation management and stakeholder engagement. Max Heinemeyer, previously VP of Cyber Innovation, took the position as Chief Product Officer in August 2022.

Denise Walter joined as Chief Revenue Officer in February 2023. Denise brings a track record of driving successful sales growth at blue-chip software businesses over more than 25 years, most recently at VMWare, and is responsible for all aspects of revenue generation, including new business growth. Finally, in June 2023 Chris Kozup joined from Zscaler as Chief Marketing Officer. Chris is an industry veteran and brings proven experience of leading high-performing marketing teams at fast-growing enterprise technology companies. Additional senior hires were made in the go-to-market and marketing teams, of people with deep experience in global partner organisations, customer success, large enterprise sales, corporate marketing and field marketing. Darktrace will continue to hire to enhance our capabilities, but now has a brilliant team in place that brings together deep experience in running successful, high-growth, innovative technology companies and is well-placed to leverage its unique technology and market positioning.

Future developments

The market opportunity ahead is enormous - over 150,000 companies that could benefit from Darktrace's AI - and Darktrace has the right team and skills in place to ensure it can go after the market opportunity that they represent. All the investments made in FY 2023 have laid the foundations for the next phase of growth and Darktrace's resilient business model means that it has the resources to support these ongoing investments as management continues to scale the business. Darktrace is prepared for this pivotal moment in the technology sector and believe that its AI-powered technology has never been as important to its customers as it is in this generative AI era. Management will continue to enhance security teams as they face new and evolving threat landscapes, enabling them to focus on what they do best - delivering their own products and services to their customers.

In balancing ongoing macro-economic uncertainty with early signs of recovery, and reflecting the time expected to see a benefit from recent investments in its Go-To-Market (GTM) strategy and teams, Darktrace is framing FY 2024 in terms of first half stabilisation and second half re-acceleration. Expecting growth to be more second half weighted than is typical has an impact on Darktrace's revenue growth, as a larger number of contracts are likely to be generating revenue for a smaller portion of the year.

Of the changes made to Darktrace's commissions structures, the most financially impactful is the decision to pay 100% of sales commissions up front, a change from past practice where 50% of commission was paid up-front with the remaining 50% typically paid one year later. This change has been made to better align with market practice, better supporting Darktrace's ability to hire and retain key experienced talent.

From a cost recognition perspective, however, Darktrace will now capitalise substantially all sales commissions and recognise them over the lives of the related contracts, unlike under past plans where it capitalised the first 50% but expensed the second 50% typically over the first year. Generally, this has the effect of moving more commission cost recognition to later periods, better aligning with revenue recognition. However, Darktrace notes that FY 2024 will be a transition year as it will still be accruing remaining portions earned, and paying out mostly all, of the second 50% of commissions it owes under FY 2023 plans.

With 100% of commissions now being capitalised, and after reviewing comparable peer practices, Darktrace has determined that to be prudent, and to better align revenue, profitability and cash flow measures for its next phase of growth, it will change its definition of Adjusted EBITDA[1] to treat all amortisation of commissions as though they were cash costs. While changes to commissions payout timing and its Adjusted EBITDA definition are resetting its baseline, underlying performance trajectory is not changing.

Business Model

Product: Create unique, efficiently developed cybersecurity products based on proprietary AI innovation

[1] Beginning in FY 2024, Adjusted EBITDA is the Group's earnings before interest, taxation, depreciation and amortisation, adjusted to include appliance depreciation attributed to cost of sales and amortisation of capitalised commissions, and adjusted to remove uncapitalised share-based payment charges and related employer tax charges, as well as certain one-off charges including the impairment of right-of-use assets.

Darktrace takes a fundamentally different technology approach – it brings self-learning AI to an organisation's unique data, rather than trying to apply AI trained on pre-existing, summarized data from multiple sources. By having the AI learn the business, not the attack or attacker, it can identify novel and insider threats that get past other traditional cyber defences.

Using a self-learning approach allows Darktrace's products to:

- Be developed efficiently and cost effectively, allowing faster roll-out of new products in response to a changing threat landscape and investment across a broader portfolio of potential new solutions;
- Learn autonomously and respond immediately, much faster than a human security team could; and
- Maintain themselves, eliminating the need for continual resource-heavy and time-intensive updating as new threats emerge.

This differentiated technology approach also means that Darktrace products provide significant value in the security stack for organisations of almost any size, industry, geography and digital complexity. The number and breadth of customers that now use Darktrace's products also allows Darktrace to better "learn how the software learns". While Darktrace does not use or share its customers' data, observing how the software evolves in response to what it encounters enables Darktrace to continuously improve its base models and make the software more effective across all environments.

Positioning: Leverage differentiated technology to drive product adoption and sales growth, across existing customers and new prospects

In a market dominated by products that use information about known threats, attacks and attackers to protect an external security perimeter, there is little to address the next logical question – what happens when something gets in? With its differentiated technology approach, and ability to look at data from any source, Darktrace products fill that gap in the cybersecurity market, but more importantly, a gap in most organisations' cybersecurity protection.

External security perimeters are usually protected by multiple products that each focus on one or more points of entry. But once a threat breaches that perimeter, or if it is from a malicious insider, where the threat came from is irrelevant; where it is going is what matters. Darktrace customers can purchase and deploy products to cover any or all aspects of their digital environments, protecting them as threats try to move from point of origin to point of attack.

By having no pre-conceived notions of the origin, entry point or shape of any threat, or how it is moving within that digital estate, Darktrace's AI is able to see and respond to anomalies that AI trained on large data sets cannot. Because Darktrace's AI takes an incremental approach – recalibrating its threat assessment quickly as an event evolves – and then quarantines just that threat, it allows all normal business activity to continue uninterrupted and gives security teams the time to investigate.

People: Hire and retain top talent to drive innovation and business success

Darktrace seeks out bright, motivated individuals with a passion for its mission and technology. It recruits across a broad range of disciplines, skill sets and experience levels and believes in bring together problem solvers who can approach challenges from a variety of different angles. By combining people with a variety of capabilities is essential for AI innovation, Darktrace takes this approach across its business, not just within its R&D centre. Fresh insights make for a better business everywhere.

Darktrace also believes that by working with people of diverse demographic and academic backgrounds, training, professional experiences and viewpoints, its employees learn more, broaden their capabilities and expand their career horizons. It is also committed to expanding the availability and diversity of technology and innovation-related talent in its markets, as well as creating desirable career paths for its current and future workforce.

Performance: Drive growth, profitability and cash flow for re-investment in the business and returns to stakeholders[2]

Product, Positioning and People all contribute to enabling continued, sustainable growth and strong business performance. Some of the key benefits to its strategy and operating model are:

- With its products applicable to a wide range of organisations, Darktrace estimates that its Total Addressable Market (TAM) encompasses over 150,000 potential customers globally[3], creating a long sales runway and the opportunity for deep product penetration;
- Products can be sold both directly to end-users and through channel partners, expanding the opportunity to penetrate the wide pool of prospects across its multiple geographic regions, industry verticals and sizes of organisation;
- Darktrace's AI gains a deeper understanding of an organisation the longer it is deployed. This results in customers purchasing products under multi-year contracts, providing Darktrace with a large amount of contracted future revenue, which creates high revenue visibility, supports attractive margins and enables the ability to invest for the longer term; and
- Combining innovative products with an efficient operating model drives cash generation, allowing Darktrace to reinvest into its Product, Positioning and People to create and sell new innovative products for further growth and profitability. This is a resilient business model that can withstand short term macro-economic pressures and other potential business

[2] Stakeholders are described on page 18

[3] For more details see the Market Overview in next section.

interruptions while continuing to invest for future sustainable growth.

Market overview

At the intersection of AI and cybersecurity

As always, the technological landscape in which Darktrace operates continues to evolve. Since its founding, Darktrace has had the mission of freeing the world from cyber disruption. While it could be said that this mission is shared by many, the approach Darktrace has taken is unique; based on the use of Artificial Intelligence ("AI") as a tool to mitigate risk and improve cyber resilience.

Many forms of AI have long been deeply integrated into daily life, embedded everywhere from tools used by individuals to power search engine results and language translations, to business applications that streamline inventory management and manufacturing processes. While this technology has had useful applications for decades, FY 2023 marked a step function increase in the mainstream awareness and use of AI.

This followed the release of Open AI's ChatGPT, and similar tools like Google Bard, which are AI and natural language processing chatbots that use large language models ("LLMs") to provide human-like responses to prompts. These generative AI technologies are tools that can be used to enhance productivity, but applied in the wrong way, could also be used for malicious or nefarious intent.

As such, the relevance of AI within the cybersecurity domain has increased significantly. This is due to the fact that generative AI can be used in various ways to launch or propagate attacks on businesses from external threat actors. However, many organisations are equally concerned with the less malicious, but potentially equally damaging, effects of unaware employees seeking to use generative AI-based tools for the improvement of everyday tasks. By uploading sensitive company data to these tools, employees can inadvertently expose the business to threats or provide sensitive data to those who may seek to misuse it.

For example, Darktrace data indicates 74% of its active customer deployments have employees using generative AI tools. This requires organisations to address the new reality that employees can now put sensitive commercial data into a tool for the purpose of having that tool write in-context responses for them, but by doing so, expose that sensitive data to public databases. At one customer, Darktrace detected and prevented an upload of over 1GB of sensitive commercial data to a generative AI tool. With this type of protection in place, Darktrace customers can allow their employees to access the benefits generative AI tools provide, while remaining protected against the potential security, IP, confidentiality and privacy risks that could follow.

Many significant impacts from the use of generative AI technology are being seen in cybersecurity. The United Kingdom National Cyber security Centre has warned that cyber criminals are using LLMs to help write convincing phishing emails in multiple languages. Darktrace has already seen examples of this this within its customer deployments. In March 2023, just after ChatGPT became mainstream, Darktrace reported an increase in social engineering email attacks, using increasing linguistic sophistication to make it harder for users – and security tools trained on known data for signature-based detection – to differentiate between a legitimate message and malicious phishing.

It's against this industry backdrop that Darktrace is set up for the next phase of growth. As the leader in the application of AI to solve cybersecurity challenges, Darktrace is uniquely positioned to help educate on and resolve the challenges associated with AI and novel threats. While the threat landscape continues to be diverse, with AI-based threats representing only a fraction of the entire threat landscape, organisations require an approach that is no longer reliant on known data or signature-based detection. If one thing has changed, it's the fact that AI can now propagate threats in machine-time versus human-time. As such, only those offerings rooted in the ability to use AI for the detection of novel threats can answer the customer need. Darktrace technology is specifically designed to detect and respond to novel, never before seen threats at machine speed – exactly the scenario that is now emerging.

Cybersecurity Policy and Spending

Globally, governments are looking to meet the challenges posed by the increasing threats of cyber disruption, particularly when attacks have the potential to cripple critical infrastructure or other functions of society.

In November 2022, the UK government announced plans to strengthen Network and Information Systems ("NIS") Regulations[4] to help protect essential digital services from what the Department for Digital, Culture, Media & Sport ("DCMS") described as "increasingly sophisticated and frequent cyber-attacks both now and in the future".

Updates to the NIS regulations apply to critical service providers such as energy providers and the National Health Service ("NHS"), along with key digital services including providers of cloud software services and online search engines. The changes

---

[4] https://www.gov.uk/government/news/cyber-laws-updated-to-boost-uks-resilience-against-online-attacks

form part of the UK government's £2.6 billion National Cyber Strategy, which aims to take a stronger approach in getting at-risk businesses to improve their cyber resilience.

In March 2023, the United States government also introduced a new cybersecurity strategy, citing how "a rapidly evolving world demands a more intentional, more coordinated, and better resourced approach to cyber defense"[5]. One of the key pillars of the Biden-Harris administration's National Cybersecurity Strategy is ensuring the defence of critical infrastructure by strengthening minimum cybersecurity requirements in sectors critical to national security. The Strategy also places a heavy emphasis on investment in secure and resilient next-generation technologies and infrastructure, along with cybersecurity research and development ("R&D") to ensure the resilience of systems in the future and has established public-private partnerships to aid in this effort.

Over the past year, the European Union has also introduced legislation strengthening cybersecurity rules affecting hardware and software products. The European Cyber Resilience Act[6] ("CRA") introduced mandatory cybersecurity requirements for manufacturers and retailers of internet enabled products, ranging from Internet of Things ("IOT") devices to software.

These policy developments across Darktrace's key customer markets, have increased the urgency for organisations of all types and sizes to invest in robust cyber tools and defend against an increasingly sophisticated and rapidly evolving threat landscape. This is the landscape Darktrace has been designing and delivering protections for since its inception, and its technology has been, and will continue to be, designed to handle this ever-increasing complexity.

<u>Darktrace uniquely positioned to protect against evolving threats</u>

Darktrace believes that the impact of AI on cybersecurity can and should be a net-positive one. That is why Darktrace has been at the forefront of 'Cyber AI' R&D since it was founded in 2013. Its use of self-learning AI to combat the most unique and hard-to-detect threats has now been in production use by close to 9,000 organisations worldwide.

Yet, not all AI is created equally. As a pioneer in the use of 'Cyber AI' technology, Darktrace has understood that the best approach to leveraging AI to combat cybersecurity challenges is an AI model that is specifically trained on the unique data of each individual business.

Known attack and signature-based security solutions are not enough

One of the most common approaches used in cybersecurity today uses large volumes of known attack data and attacker behaviour to establish signature-based detection of threats. These models often use supervised machine learning – meaning that the AI identifies patterns, but humans interpret that data and develop the response -- and are common in modern extended detection and response ("XDR") solutions. These techniques perform well at stopping attacks that have been around for long enough, and in consistent enough form, to be recognisable. While this functionality served a purpose, the advent of threats now generated in machine-time renders this approach inadequate for the current threat landscape. There are frequent examples of novel threats getting past these defences and doing material damage to businesses, governments, and other entities. As long as attackers continue to innovate (and especially now that generative AI tools can provide a faster, easier, almost continuous process of launching attacks) solutions based solely on known attack data and signature-based detection are not enough.

Darktrace's Self-Learning AI – a fundamentally different approach

Darktrace uses self-learning AI, which is designed to – without human intervention –gain an understanding of the organisation's behavioural patterns (e.g. for every user, device, endpoint, app and interaction). It is trained on these patterns in real time from the richest, most granular and most relevant data available – the unique data of the organisation. Because it is not focussed on known attack patterns but on detecting when something is not right, it can spot and quarantine novel threats like zero day, insider, nation-state attacks. And because self-learning AI eliminates the lag time inherent when humans must be involved, it protects against even generative AI attacks like sophisticated phishing attacks at scale or evergreen novel threats.

Recent advances in generative AI are being heralded as an important new addition to the growing arsenal of AI techniques that will transform cybersecurity. However, Darktrace has been using forms of generative AI, including LLMs, across its products since inception. For example, Darktrace's Cyber AI Analyst uses generative AI techniques to perform real-time analysis, and write immediate, natural language reports of incidents helping security staff to remain informed and armed with the best approach for remediation.

Darktrace technology is unique in its ability to understand and detect novel attacks, especially as generative AI allows such attacks to be faster and more frequent, making it a must-have in any security stack. While self-learning, or indeed any AI, is unlikely to replace all human effort in cybersecurity, it can help employees work smarter and more effectively.

---

[5] https://www.state.gov/announcing-the-release-of-the-administrations-national-cybersecurity-strategy/
[6] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Challenging economic environment

The rapidly evolving AI landscape over the past year has been set against an economic backdrop coloured by the impact of Russia's invasion of Ukraine, a resulting energy crisis, high inflation, and elevated debt levels resulting from the COVID-19 pandemic. As global economies have seen downturns, and as the prospect of a global recession loomed[7], countries, businesses and individuals have seen their budgets squeezed.

This macro-economic backdrop has affected every sector, and the cybersecurity sector has not been immune – although notably less impacted compared with other sectors of IT. Darktrace, like many of its peers, has experienced increased customer scrutiny when it comes to the trial and subsequent procurement of new solutions.

Darktrace responded to the first signs of economic uncertainty by taking a prudent approach to managing discretionary costs. Combined with a strong cash position and contracts that average over 36 months in length providing additional revenue and cash flow visibility, Darktrace was able to continue investing in its product development, go-to-market strategy and its employees to ensure that it can emerge in the best possible position to capitalise on the significant opportunity ahead.

Darktrace's approach to its addressable Market

A large part of capitalising on the available opportunity, whether now – in a more challenging economy – or through and beyond economic recovery, is making sure that Darktrace's go-to-market organisation is appropriately experienced and enabled to communicate the unique value of Darktrace's expanding product set. Denise Walter joined Darktrace as Chief Revenue Officer in February 2023, bringing long-term experience in large enterprise software sales. She has set a path for maturing the sales teams, enabling increased sales across larger organisations in the strategic segment, evolving the business's channel strategy and ensuring a seamless and supportive experience across the customer lifecycle. She has brought in experienced sales, channel, and customer success executives to help her drive this evolution and is a driving stakeholder in Darktrace's next steps to improve the data and systems necessary to make reliable prospect, customer, contract, and operating information readily available to support the sales and ongoing customer experience.

Also, late in the financial year, Chris Kozup joined Darktrace as Chief Marketing Officer, bringing significant experience in business to business ("B2B") enterprise marketing within the cybersecurity, cloud and networking sectors. Chris has also started to expand the marketing organisation with strategic leadership hires to augment capabilities in brand, demand generation, product and solutions messaging and positioning.

Having hired these two positions from the pool of experienced talent in the United States, Darktrace has moved further towards its goal of accelerating penetration in the large North American market. The United States is not only Darktrace's single largest revenue market but is also its single largest untapped opportunity. By hiring its senior market-facing leadership in the United States and building teams with experience and existing networks there, Darktrace is investing in its belief that North America can be a significantly larger market for its products than it has capitalised on to date.

In both the sales and marketing functions, leadership is strengthening marketing segmentation, improving understanding of different needs, and enabling communications that speak to those. While there are some teams that focus on industry verticals, particularly critical infrastructure, size of prospect and customer continues to be the primary basis for Darktrace's market segmentation Darktrace's AI platform can be applied to companies of almost all sizes, across all sectors and geographies and is complementary to more traditional security solutions available in the broader market.

Darktrace operates within the Information Security and Risk Management market, which Gartner, a global research and advisory company, estimates to amount to approximately $188.1 billion (2023 estimates)[8] . The Information Security and Risk Management market comprises Application Security, Cloud Security, Data Privacy, Data Security, Consumer Security Software, Identity Access Management, Infrastructure Protection, Integrated Risk Management, Network Security Equipment, Security Services, and Other Information Security Software. Gartner estimates the total market will see a compound annual growth rate of 11.0% from 2022 to 2027 on a constant currency basis.

Darktrace estimates its total addressable market ("TAM") using both a bottom-up approach based on addressable global companies and their potential adoption of Darktrace's offering, as well as a top-down approach based on the overall cybersecurity market size. Darktrace currently estimates that that there are approximately 150,000 companies[9] – more than 15 times its current customer base – in its current and potential markets that could benefit from its security technology. Additionally, there are significant opportunities to expand product penetration within Darktrace's existing customer base,

---

[7] https://www.weforum.org/press/2023/01/chief-economists-say-global-recession-likely-in-2023-but-cost-of-living-crisis-close-to-peaking/

[8] Shailendra Upadhyay, Christian Canales, Ruggero Contu, Lawrence Pingree, Elizabeth Kim, Swati Rakheja, Rustam Malik, Nat Smith, Rahul Yadav, Mark Wah, Akshita Joshi, Matt Milone, Mark Pohto, Sean O'Neill, Travis Lee, Dan Ayoub (2023) Forecast: Information Security and Risk Management, Worldwide, 2021-2027, 2Q23 Update, Gartner

[9] The figure of 150,000 addressable companies is defined as being those that have more than 250 employees globally, compared to Darktrace's roughly 8,800 customers as of 30 June 2023 (addressable global companies based on OECD, Eurostat, US Bureau of Labor Statistics, and UK Office for National Statistics, excluding China or Russia).

by expanding coverage either as customers grow or to more areas of their digital estate by upselling existing and new products and solutions. Darktrace estimates that in total, its opportunity value could be approximately $48 billion, reflecting a substantial global greenfield and product penetration opportunity.

And while Darktrace remains focussed on capturing the large available opportunity in the cybersecurity markets - at least in the short-to-intermediate term - its self-learning AI technology has broader application in tangential areas like data centre management and IT governance. Darktrace also believes that as generative AI gains acceptance and its uses become better understood and its risks better managed, the potential applications for Darktrace's technology can increase significantly. Darktrace has been planning for this evolution of AI technology for over a decade and believes that it is uniquely positioned to capitalise on current and upcoming change – both in cybersecurity and beyond. At its core, Darktrace is not a cybersecurity company that leverages AI, it is an AI company that currently focuses on the large opportunity in cybersecurity.

Darktrace innovations

Self-Learning AI

Self-Learning AI sits at the heart of Darktrace's technology differentiation.

A foundational part of how Darktrace protects its customers is by training on the uniqueness of their individual environments. No two organisations are the same, and their security solutions should be able to adapt to the specific requirements of each.

The Only True Self-Learning Cyber AI

- AI that trains on the uniqueness of each individual organisation.
- Designed to address the challenges of Generative AI-based threats by pitting AI against AI.
- Takes a self-learning approach that is always on, always learning, always improving.
- Allows for the reduction of cost through the consolidation of legacy security tools.

Active, Reactive and Proactive

- Delivers active, reactive and proactive cyber threat capabilities in a feedback loop that continuously learns and enforces normal.
- *Autonomously detects, contains and disarms threats, all supported by AI-driven threat analysis.*
- Enables security teams to identify vulnerable attack pathways and proactively protect critical assets.
- Empowers informed human decisions for restoring assets already compromised.

Anywhere, Everywhere and Everyone

- Monitors and protects all digital assets across the entire organisation.
- Provides end-to-end cybersecurity coverage, including Network, Email, Apps, OT, and Cloud for a single, holistic picture of the entire environment.
- Lives in any environment, big or small, simple or complex, across all industries. Learns any type of organisation, from SMBs and enterprises to critical infrastructure and government.

Make Humans Better at Cybersecurity

- Supports human performance with AI coverage of digital ecosystems at a scale far beyond human purview.
- Leverages human skills with autonomous AI information.
- Improves decisions and outcomes based on total visibility into the digital ecosystem.
- Empowers security teams to be proactive with AI Adversary tools, as well as gain agility in the recovery process.

The Darktrace portfolio

Darktrace's vision is to free the world of cyber disruption. To do this, Darktrace has developed the use of self-learning AI applied to the challenges of cybersecurity. This core engine of self-learning AI is unique in that it is trained on each customer's actual IT and business environment. By doing this, Darktrace has the ability to identify and take action on both existing and emerging threats in a way that other solutions simply cannot do.

From a product portfolio perspective, Darktrace takes a platform approach to cyber resilience by applying its self-learning AI engine across critical IT domains, as follows:

- Network;
- Cloud;
- Endpoint;
- Zero Trust;
- Email;
- SaaS;
- Operational Technology (OT)

The uniqueness and strength of Darktrace's approach is in its ability to take action on new and existing threats (including those generated by AI) while extending this across every part of a company's digital estate. Furthermore, because the AI engine is shared across each of these domains, Darktrace has the unique ability to enhance visibility and strengthen actions across each domain. For example, Darktrace can correlate a security incident that occurs in email with what is happening on the network. Or, Darktrace can ensure a consistent defence across network to cloud. Essentially, Darktrace can provide a completeness of cyber resilience across the entire organisation with a more hardened defence due to being able to triangulate and correlate insights from each domain.

Coverage areas
Darktrace technology can be brought to any environment, protecting cloud infrastructure – from AWS to Microsoft Azure – the full range of SaaS applications, endpoints, zero trust technologies and IT/OT networks.

Embrace the Benefits of Cloud, Without Taking on the Risks
Delivers the only cloud cybersecurity solution that provides complete visibility into the cloud footprint, detects and responds to novel threats, and ensures the correct posture and entitlements for cloud workloads.

Interrupt SaaS Application Misuse
Understands users' patterns across every application an organisation uses to spot behaviour that doesn't belong, from compromised credentials to malicious insiders.

Neutralise the Full Range of Email Attacks
Understands email users and how they communicate to spot and stop email threats. Protects against Microsoft 365 account takeovers and prevents accidental data loss from misdirected emails. Educates and engages employees in email security. Boosts productivity by sorting non-productive mail.

Protect your Workforce, Everywhere
Analyses rich, host-level data via Darktrace agents or EDR integrations, enhancing threat protection across the dynamic workforce, on or off the VPN.

Shut Down Network Threats Instantly
Learns normal 'patterns of life' to discover unpredictable cyber-threats across the corporate network, and then takes targeted action to minimise disruption. Detects and responds to ransomware at every stage.

Complement and Enhance Zero Trust Policies
Validates the organisation's zero trust policies and informs future decision-making with always-on, real-time visibility into every system and asset.

Light up your Industrial Environment
Passively learns repetitive as well as evolving ICS behaviour to protect the business from known and unknown OT and hybrid IT/OT threats. Protocol agnostic.

In addition to this completeness of coverage, Darktrace also provides a complete lifecycle of cyber resilience including the ability to prevent attacks, rapidly detect them when they do occur, automate the response, and finally recover rapidly once a breach has occurred. Darktrace customers benefit from a core AI platform approach across their entire organisation combined with a 360 degree life-cycle readiness that is defined as: PREVENT, DETECT, RESPOND, HEAL Coverage areas. Darktrace technology can be brought to any environment, protecting cloud infrastructure – from AWS to Microsoft Azure – the full range of SaaS applications, endpoints, zero trust technologies and IT/OT networks.

PREVENT
Prioritise threats. Harden Defences. Reduce risks.
Darktrace PREVENT allows the security team to identify, prioritise, and test vulnerabilities, reducing risk and hardening defences both inside the organisation and outside on the attack surface - continuously and autonomously.

Darktrace uses AI to "think like an attacker", finding pathways to an organisation's most critical assets from inside and outside. And it continuously analyses the most disruptive attacks on an organisation and feeds that information back into DETECT + RESPOND.

The PREVENT product family consists of two products:
- PREVENT/Attack Surface Management (or ASM), which continuously monitors a business' attack surface for known and unknown external risks, and
- PREVENT/End-to-End (E2E), which hardens defences internally, testing and prioritising the most critical attack paths.

PREVENT/ASM
Darktrace PREVENT/Attack Surface Management™ continuously monitors an organisation's attack surface for risks and high-impact vulnerabilities digitally exposed to the outside world, offering an outside-in perspective.

It uses AI to understand what makes an external asset "yours" for a business, searching beyond known servers, networks and IP.

Within the PREVENT/ASM capability sits Darktrace Newsroom, launched in February 2023 which keeps security teams informed of newly discovered critical vulnerabilities and supports timely mitigation actions to prevent exploits.

PREVENT/E2E
Darktrace PREVENT/End-to-End delivers a set of five capabilities based on new AI algorithms developed by researchers at the Darktrace AI Research Centre in Cambridge, UK to help organisations pre-empt attacks.

- *Attack Path Modelling*: A revolutionary approach to mapping the most impactful attack paths through an organisation in real-time. Crucial support for that modelling comes from Darktrace Self-Learning AI, which provides a continuous understanding of the most vulnerable and valuable paths across the digital ecosystem.
- *Pentest Augmentation*: Does what traditional human and conventional Red Teaming cannot: tests all potential attack pathways around-the-clock and analyses every touchpoint across the digital ecosystem.
- *Breach & Attack Emulation*: Emulates how an adversary might attack. Security teams can deploy harmless "attacks" that emulate malware, phishing, spoofing, and other common threats. Automatically monitors for unsafe testing by auto-switching to a theoretical attack if necessary.
- *Security Awareness Training*: Identifies users who are exposed or potentially prone to phishing, allowing IT teams to tailor training based on real world data. The product mimics the best attackers to test human defences and incident response processes.
- *Cyber Risk Prioritisation:* Enables the security team to harden defences with a prioritised list of vulnerabilities - complete with suggestions about how to harden them. Combined with Darktrace DETECT + RESPOND, it autonomously implements countermeasures to ensure critical vulnerabilities and attack paths can't be exploited and cause damage.

DETECT
See attacks instantly
Most cybersecurity vendors claiming to use AI rely on identifying threats based on historical attack data and reported techniques. In contrast, Darktrace DETECT delivers instant visibility into threats – even the most advanced threats, novel malware strains, and new techniques – by knowing what's normal, to identify what's not.

Darktrace DETECT learns from the organisation's data.

It detects cyber-threats not because it has seen them before, but because they represent a departure from an organisation's normal activity. It learns what makes an organisation unique, from the ground up and without any prior assumptions as to what constitutes a threat. This understanding allows it to detect subtle patterns that reveal deviations from the norm, making it possible for the security team to identify attacks in real time, not after the damage has been done.

The solution feeds data into Darktrace RESPOND to disarm threats that could disrupt operations.

Darktrace DETECT works across the entire digital ecosystem, wherever an organisation's data resides – from cloud infrastructure and applications to email systems, endpoints, zero trust technologies, on-prem networks and Operational Technology ("OT").

RESPOND
Disarm within seconds
Darktrace RESPOND delivers autonomous, always-on action to contain and disarm attacks within seconds. When a threat is detected, Darktrace RESPOND leverages Darktrace's understanding of "self," bespoke to each organisation, to pinpoint signs of an emerging attack, interrupting malicious or dangerous activity, while allowing normal business to continue. It works with precision, targeting actions tailored to the threat.

Because Darktrace RESPOND doesn't rely on pre-programming, threat characteristics are not defined in advance.

This enables it to neutralise unknown and unpredictable cyber-attacks that have never been seen before on the first encounter, before damage spreads.

Darktrace RESPOND takes action either via integrations into an organisation's existing security controls, allowing the CISO and security team to leverage and supercharge existing investments, or through native response mechanisms. Integrations allow Darktrace RESPOND to reach every corner of the business from cloud systems and endpoints to zero trust technologies.

The AI technology runs autonomously at all times, elevating humans from making micro-decisions about individual events to making "decisions about decisions" – setting parameters for the solution to act, and then allowing the AI to do the heavy lifting. Darktrace RESPOND acts within guidelines and boundaries set by the security team.

HEAL
Be ready, recover quickly

Darktrace HEAL, which became generally available in August 2023, uses AI to understand a business's data to ensure readiness to recover from an active cyber-attack and to rapidly restore the business to an operational state.

It enables organisations to determine the least disruptive way to eradicate the threat, recover to an operational state, and strengthen and adapt that organisation's security posture to harden against repeat or similar offenses.

Darktrace HEAL is designed to become more valuable and effective as the complexity of the incident increases. It achieves this by deeply understanding the organisation, its assets, and the full range of security events that can occur.

By having this understanding, Darktrace HEAL can adapt its recovery decisions to provide the most ideal path to recovery. Moreover, Darktrace HEAL also reduces the time needed to restore the organisation to a fully operational state after an incident occurs. The product/capability leverages its knowledge about the organisation and its security events to make the best recovery decisions. This ultimately leads to quicker recovery, resource savings, and a faster restoration of normal operations for the company.

AI ANALYST

Explainable AI Cyber

AI Analyst investigates threats throughout the cycle, delivering readable reports to keep the human updated. It creates the interface between the AI technology and human decision making.

Cyber AI Analyst optimises threat investigation by continuously examining every security threat that arises. It spotlights the highest priority threats at any one time and rapidly synthesises all of the context around an attack into a natural language report.

The result is that time-to-meaning and time-to-response are dramatically reduced – allowing security team members time to use their expertise where it really matters.

DARKTRACE SERVICES

An extension of your team

Darktrace is committed to ensuring that its customers receive the maximum value from Darktrace's Self-Learning AI technology and expert analysts. Darktrace's bespoke service options can be customised around Darktrace's offerings to uplift and augment security teams. Services are delivered by Darktrace's dedicated Cyber Analysts, Cyber Technicians and the Darktrace 24/7 SOC operation, comprised of experts in threat analysis and risk mitigation. Most importantly, these offerings are crafted based upon Darktrace's extensive experience working with over 8,700 customers of every size and across every industry – it is this expertise that allows Darktrace to provide services that are tailored to any organisation.

Proactive Threat Notification (PTN)

Proactive Threat Notification (PTN) provides comprehensive threat notification around the clock. Cyber Analysts in the global Darktrace Security Operations Centre (SOC) triage high-priority DETECT alerts within a customer's digital ecosystem – helping investigate the alert, jumpstarting the remediation process, and boosting the customer security team with additional expertise when they most need it.

Ask the Expert (ATE)

Ask the Expert (ATE) gives the customer's security team 24/7 access to expert Darktrace Cyber Analysts. Customers can send queries if they need assistance during live threat investigations, or even during day-to-day operations, and receive rapid feedback. Collaborating with Analysts through the service ensures customers are benefitting from the latest understanding of the threat landscape and getting the best possible support.

Key performance indicators (KPIs)

KPIs are financial and non-financial measures used by Darktrace Management, its Board of Directors, its investors and other stakeholders, to assess business performance, monitor principal risks and evaluate future expectations.

Management and the Board believe that Adjusted EBITDA margin is a useful measure of underlying operating performance, alongside other KPIs such as Operating profit margin (EBIT) and Adjusted EBIT margin. Adjusted EBITDA excludes certain items, such as share-based payment and related tax charges, certain depreciation and amortisation that are not indicative of, or that may impair the period-to-period comparability of, Darktrace's core operating performance. Darktrace uses Adjusted EBITDA margin as its primary profitability measure when developing its internal budgets, forecasts and strategic plan, in analysing the effectiveness of its operating performance, and in other strategic assessments and communications. In prior years, Darktrace also presented EBITDA, but has now determined that it does not add significant value beyond that provided by the combination of Adjusted EBITDA, Adjusted EBIT and core IFRS measures, including Operating profit (EBIT).

Most, but not all, KPIs are Alternative Performance Measures (APMs), which are not defined under IFRS and are not intended to be a substitute for any IFRS measures of performance; wherever appropriate and practical, Darktrace provides reconciliations of its APMs to relevant IFRS measures. APMs are developed and presented as Management and the Board consider them to be important supplemental measures to enhance stakeholders' understanding of business growth, underlying profitability, and other business performance and trends. APMs do not have standard definitions and therefore may not be comparable to similar measures presented by other entities. Additional group APMs are disclosed in the consolidated accounts of Darktrace plc publicly available: https://ir.darktrace.com/financial-results.

Adjusted EBITDA and margin

$'000	FY 2023	FY 2022	% change
Adjusted EBITDA	105,012	68,058	54.3%
Adjusted EBITDA margin (%)	19.3%	16.4%	2.9ppt

Definition and relevance
Darktrace's Adjusted EBITDA is earnings before interest, taxes, depreciation and amortisation, adjusted to include appliance depreciation attributed to cost of sales, and to remove uncapitalised share-based payment (SBP) charges and related employer tax charges, as well as certain one off charges including the impairment of right-of-use assets. Adjusted EBITDA as a percent of revenue is the Adjusted EBITDA margin.

Due to the unpredictable nature of these non-cash charges, and that SBP related employer tax charges are driven by movements in share price and are therefore outside of Darktrace's control, these costs are excluded in the calculation of Adjusted EBITDA. Management believes that this treatment improves the ability to make period-to-period comparisons of core operating performance and is consistent with treatment applied by listed European and US software peer companies.

For the calculation of this measure, Darktrace treats the appliance depreciation reflected in cost of sales as though it were a current period cash cost. As Darktrace is unusual in supporting on-premise software deployments with appliances that it owns, maintains and reuses over their useful lives, this treatment provides better comparability to software companies that sell hardware to support similar deployments and recognise those direct cash costs.

Performance
Year-over-year, Adjusted EBITDA increased by $37.0 million, resulting in a 2.9 percentage point increase in Adjusted EBITDA margin to 19.3%.

Reconciling Operating profit (EBIT) to Adjusted EBITDA for FY 2023, Darktrace added back $64.2 million in net non-cash depreciation and amortisation charges, an increase of $13.0 million in the period. In its calculation of Adjusted EBITDA Darktrace does not add back to operating profit the $16.7 million of appliance depreciation included in Cost of sales which relates to appliances used to deploy software at customer sites. For FY 2023, there was a $2.1 million year-over-year increase in depreciation of appliances in Cost of sales, reflecting new, on-premise customer deployments. Appliance depreciation attributed to Cost of sales grew more slowly than might first be expected considering Darktrace's revenue growth as more customers choose to have products deployed virtually, and as Darktrace sells more products that are only deployed virtually.

Darktrace also added back $26.5 million in net SBP and related employer tax charges, a decrease of $2.2 million in the period. This decrease was due to a $6.0 million decrease in SBP cost, partially offset by a $3.9 million decrease in SBP related tax charges, due to the increase in share price. The Company also added back a right-of-use asset impairment charge of $1.8 million reflecting its current assessment of the cost it will incur to exit a lease contract on now-unused office space.

Reconciliation of Net Profit to Adjusted EBITDA

$000	FY 2023	FY 2022	% change
Revenue	542,807	414,123	31.1%
Net Profit	**37,070**	**(2,027)**	**n/a**
Taxation	(8,931)	2,090	-527.3%
Finance income	(3,247)	(188)	1,631.7%
Finance cost	4,291	2,879	49.0%
Operating profit (EBIT)	**29,182**	**2,754**	**959.6%**
Operating profit margin	**5.4%**	**0.7%**	
Depreciation & Amortisation	64,239	51,242	25.4%
EBITDA	**93,421**	**53,997**	**73.0%**

$000	FY 2023	FY 2022	% change
EBITDA	**93,421**	**53,997**	**73.0%**
Appliance depreciation in cost of sales	(16,668)	(14,589)	14.3%
Impairment of right-of-use asset	1,781	-	n/a
Share-based payment (SBP) charges	22,340	28,410	-21.4%
SBP related employer tax charges	4,139	241	1,614.6%
Adjusted EBITDA	**105,012**	**68,059**	**54.3%**
Adjusted EBTIDA margin	**19.3%**	**16.4%**	**n/a**

Adjusted EBIT and margin

$'000	FY 2023	FY 2022	% change
Adjusted EBIT	57,441	31,405	82.9%
Adjusted EBIT margin (%)	10.6%	7.6%	3.0ppt

Definition and relevance

Darktrace's Adjusted EBIT is its earnings before interest and taxes, adjusted to remove uncapitalised share-based payment (SBP) charges and related employer tax charges, as well as certain one-off charges including the impairment of right-of-use assets. Adjusted EBIT as a percentage of revenue is the Adjusted EBIT margin.

Adjusted EBIT considers both cash and non-cash charges incurred by Darktrace in the period, demonstrating what underlying operating profit would have been without the impact of certain charges that are both unpredictable and outside of Darktrace's control. This includes SBP related employer tax charges which are driven by movements in share price. Management believes this treatment aids period-to-period comparison of operating performance with Darktrace's peers, and by excluding the impact of these unpredictable or uncontrollable charges, further enhances management's ability to predict and communicate Darktrace's longer-term expected 'steady state' economic model.

Performance

Year-over-year, Adjusted EBIT increased by $26.0 million to $57.4 million, resulting in a 3.0 percentage point increase in Adjusted EBIT margin to 10.6%.

Reconciling Operating profit (EBIT) to adjusted EBIT, Darktrace added back $26.5 million in net SBP and related employer tax charges, a decrease of $2.2 million in the period. This decrease was due to a $6.0 million decrease in SBP cost, partially offset by a $3.9 million decrease in SBP related tax charges, due to the increase in share price. Darktrace also added back a right-of-use asset impairment charge of $1.8 million reflecting its current assessment of the cost it will incur to exit a lease contract on now unused space.

Reconciliation of Operating profit (EBIT) to Adjusted EBIT

	FY 2023 $'000	FY 2022 $'000	% change
Operating profit (EBIT)	**29,182**	**2,754**	**959.6%**
Impairment of right-of-use assets	1,781	-	n/a
Share-based payment (SBP) charges	22,340	28,410	-21.4%
SBP related employer tax charges	4,139	241	1,614.6%
Adjusted EBIT	**57,441**	**31,405**	**82.9%**
Adjusted EBIT margin (%)	**10.6%**	**7.6%**	**n/a**

Risk

Enterprise Risk Management Framework Enterprise Risk Management ("ERM") is distilled into Darktrace's culture and is a key aspect of how the business operates. The entire business takes an active role in managing risks throughout day-to-day operations, guided by the Board and the risk parameters set out as part of Darktrace's business objectives.

Darktrace's subscribes to the ISO 3100 risk management methodology and the ERM approach to managing its risk profile, which enables it to manage all forms of risk and maintain a consistent approach in the identification, management and reporting of risks.

Darktrace's ERM framework continues to evolve as the business develops and the Principal and Emerging Risks are reviewed and updated accordingly.

Risk Governance

Board

The Board has overall responsibility for Enterprise Risk Management and setting the Group's risk appetite. It monitors the risk environment and assesses the appropriateness of risks to the business and any mitigating or management strategies.

Audit and Risk Committee

The Audit and Risk Committee plays a key role in determining the Group's risk appetite and making sure that procedures are in place for identifying, managing, and reducing the Principal and Emerging Risks of the Group and reports to the Board on ERM.

The Audit & Risk Committee evaluates the Principal Risks to determine whether they remain pertinent, efficient, and in line with achieving Darktrace's strategic goals while being within the Group's risk appetite.

Risk Steerco

The Risk Steerco is made up of representatives from across the business both functionally and geographically and is responsible for identifying and overseeing the Principal, Emerging and Business Risks.

The Risk Steerco convenes monthly, to ensure appropriate review and reporting of organisational risks to ensure that up to date information is provided to the Audit and Risk Committee.

The responsibilities of the Risk Steerco in relation to ERM include:

- evaluating and proposing to the Audit & Risk Committee appropriate levels of risk appetite and risk tolerance (i.e., acceptance of risk ratings) for the corporate level risks of the business;
- documenting policies and procedures for risk management activity;
- employee training in respect of the policies and procedures to be followed
- appropriate reporting of risk management issues to senior management, the Audit & Risk Committee and the Board;
- monitoring compliance with the ERM framework;
- delegating authority to Management, where appropriate; and
- reporting on significant risks to the Board of Directors, Audit & Risk Committee and, where appropriate, Government bodies.

Risk identification

Darktrace's risk identification process uses a "top-down, bottom-up" approach that is applied across the entire organisation. The top-down approach identifies Principal Risks that pose the greatest threat to the delivery of Darktrace's strategic objectives. The bottom-up approach identifies Strategic, Operational, Compliance, Security and Change Risks ("Business Risks") that occur at a regional and functional level.

Risk assessment
All identified risks are assessed for likelihood and impact using the ISO 3100 risk assessment methodology, which takes into account the likelihood and potential impact of the risk, e.g. to Darktrace's security, customers, employees or finances. The analysis takes into account risk both before any mitigation ("Inherent Risk") and after all existing mitigations ("Residual Risk"). This facilitates decision making with appropriate consideration of risk at all levels. The primary advantage of assessing Inherent Risk is that it indicates possible risk exposure if mitigations were to fail entirely or not be implemented.

Risk appetite
Risk appetite is how much risk exposure Darktrace is willing to accept. The Board, based on the recommendations of the Audit & Risk Committee and the advice of the Risk Steerco has defined the risk appetite level within Darktrace's ERM framework which helps Executive Risk Owners make more informed decisions on the level of acceptable risk.

Darktrace's risk appetite is set at low as outlined within its Risk Management Policy and is formally approved by the Audit & Risk Committee. Low risks are deemed to have a very low to moderate impact to Darktrace and a conceivable to possible probability of realisation.

Risk Management
Darktrace acknowledges that risk elimination is frequently neither realistic nor desirable, so it uses risk appetite to provide its leaders with guidance to support appropriate decision making in the pursuit of Darktrace's strategic goals. Ultimately, Darktrace's Board has responsibility for the ERM Framework and internal controls and the Board has given its approval to the risk appetite declaration.

All Principal risks are given an Executive Owner. The Executive Owner oversees management of the overall risk, ensuring that sufficient controls are in place and that, should a risk exceed the appropriate appetite level, the requisite action plans are implemented effectively. Principal Risks are reviewed quarterly with the assigned Executive Owner and relevant supporting business functions.

Business Risks are recognised and recorded at a regional or functional level. Reviews of business risks are completed on a quarterly cycle by the relevant functions and are also reviewed by the Risk Steerco.

Risk reporting and Monitoring
Through bottom-up risk registers that are regularly updated in Darktrace's risk and control system, global visibility of risks recognised by its regions, company departments and sectors is developed. Bottom-up risks are coupled with top-down risks using the ERM framework with the latter being recognised and owned by an Executive.

The Audit and Risk Committee is responsible for reviewing the effectiveness of Darktrace's internal controls for Principal Risks and for reporting relevant matters to the Board. The Risk Steerco ensures that Darktrace's Business Risks are comprehensive, managed, and communicated appropriately to the Audit and Risk Committee.

Whilst there is a formal process in place for reporting on risks, risks can be reported to the Board and Audit and Risk Committee outside of the established reporting cadence, should events dictate that this is necessary and appropriate.

Principal Risks
The aim of this section is to describe the principal risks and uncertainties facing Darktrace and explain how they are managed or mitigated. These are the risks, or a combination of risks that can seriously affect the performance, future prospects or reputation of Darktrace.

Inability to innovate Darktrace products – residual risk low
Failure to innovate, develop and enhance the AI Cyber Loop, to adapt to the increasingly sophisticated and changing nature of cyber-attacks posed by threat actors and the emergence of new generative AI LLMs. Darktrace may also fail to innovate against the market's current requirements and in line with Darktrace's overall business strategy.

The continuous investment and growth within R&D and the expansion of the product offering has reduced the overall residual risk.

Customer service delivery failure – residual risk medium
The Group may fail to anticipate and understand customer needs appropriately and in a timely manner, therefore risking failure to deliver value to the customers.

Go-to-Market teams are being expanded to match growth demand and processes for dealing with customer demands are being improved and automated.

Inadequate channel sales and support – residual risk medium
The Group relies on the channel i.e., third parties, including distributors, resellers, referral partners and managed service providers, to generate a significant portion of its revenue.

No change.

Cloud service providers downtime – residual risk medium
The Group relies on Cloud Service Providers, such as Amazon Web Services ("AWS") and its own data servers to host and operate an increasing number of deployments for the Darktrace product line.

No change.

Failure to retain and attract new employees – residual risk medium
The Group relies on the performance of highly skilled personnel, including key employees, to deliver on its strategic objectives.

No change.

Darktrace Cyber Incident – residual risk medium
Risk of failure of its systems and compromise of its data, through cyber-attack, cyber-intrusion, insider threats or otherwise. Failure to responsibly collect, process and store data, together with ensuring an appropriate standard of cybersecurity across the business.

Overall, the Darktrace Cyber Incident risk remains at medium to the business. The minor increase of the threat to Darktrace is due to Darktrace's expansion of its use of new SaaS vendors to enable better productivity which may introduce potential security risks. The Darktrace Security team are aligned with all new business change projects and continue to advise and monitor the introduction of new SaaS vendors vigilantly.

Intellectual property theft or exposure – residual risk medium
The Group may fail to adequately protect its intellectual property, proprietary rights and prevent others from making unauthorised use of its platform and technologies, especially at a time when competitors are embracing new generative AI LLMs.

No change.

Autonomy related matters – residual risk low
The Autonomy related litigation represents a potential risk for Darktrace from both a reputational and a legal perspective.

No change. During the period the Audit & Risk Committee approved the Risk Steerco's assessment of the overall materiality impact of the risk remains low.

Major changes
Brand & Reputation
The Audit & Risk Committee analysed the Brand & Reputation Principal Risk, and it was assessed that Brand and Reputation are risk impact factors for all risks, rather than a standalone Principal Risk. The Brand and Reputation Principal Risk has been distilled into four Business Risks that impact Darktrace's brand and reputation (Misinformation Campaigns, Market Share, Third Party Endorsement and Brand Awareness) and the Principal Risk name changed to Autonomy Related Matters.

All risks now have a reputation impact rating to help assess the materiality of reputational impact if those risks were to occur. The reputation impact rating scheme has been embedded within the ERM Framework for all risks. All Principal Risks have been assessed for their brand and reputational impact and this is monitored by the Audit & Risk Committee

Customer Service Delivery Failure
The Principal Risks 'Understanding & Responding to Customer Needs' and 'Customer Service Delivery' were combined into one Principal Risk, customer service delivery failure, as the threat and impact of the two risks were both customer focussed and posed the same potential threat to the business. The Audit & Risk Committee, with the advice of the Risk Steerco formally accepted the combination of those two Principal Risks.

Principal Risk Renaming and Restructuring
During FY 2023 Darktrace further scrutinised its Principal Risks and renamed certain of them to ensure that they reflected the true nature and evolution of the risks in relation to Darktrace as it has now developed since its IPO in 2021. The Audit & Risk Committee, with the advice of the Risk Steerco formally accepted the renaming of the Principal Risks as set out below.

New name	Previous name
Customer Service Delivery Failure	• Unable to develop Darktrace products to mitigate evolving cyber threat landscape • Insufficient customer support resources
Inability to innovate Darktrace products	Unable to meet customer requirements within the product line
Inadequate Channel Sales and support	Reliance on Partners and Resellers to generate new business
Cloud Service Providers downtime	Reliance on outsourced hosting for services
Failure to retain and attract new employees	Employee retention and recruitment
Intellectual Property theft or exposure	No change
Darktrace Cyber incident	Cyber-attack or systems failure
Autonomy related litigation	Brand & Reputation

Principal Risk downgrading
As part of the ERM Framework evolution the Principal Risks were scrutinised for their potential material impact on the business goals and a Principal Risk was downgraded to Business Risk.

COVID-19: As the world learned to deal with COVID-19 so did Darktrace. The impact of COVID-19 was assessed to no longer have a potential material financial impact on Darktrace. As such, a new Strategic Business Risk for Pandemics has been created to ensure there is resilience in the event of any future pandemics. The Audit & Risk Committee, with the advice of the Risk Steerco formally accepted the downgrading of the COVID-19 risk.

Emerging Risks
During 2023, in line with Darktrace's evolving ERM Framework, all Emerging Risks, were re-evaluated to focus on risks that could have a potential material impact on the business. This re-evaluation led to two significant changes: to the number of Emerging Risks and to the definition of an Emerging Risk. This evaluation has enabled Darktrace to better focus its mitigations on risks that are more likely to affect its business model.

Darktrace defines Emerging Risks as risks that may, in time, pose a threat to Darktrace's business model and are more unpredictable, have a greater level of uncertainty or in relation to which there may be less relevant data or detailed information available to formally assess the materiality of the risk.

Darktrace has procedures in place to identify Emerging Risks, including horizon scanning, and monitoring market and consumer trends. Darktrace also identifies Emerging Risks utilising in-house expertise that forms part of the ERM Governance structure and in turn "crowd sources" for emerging risks from its own industry experts.

Emerging Risks are reviewed quarterly by the Risk Steerco to assess their relevance, potential impact and status. Potential mitigations are prepared and if an Emerging Risk is assessed as quantifiable it is incorporated within the wider ERM Framework Risk registers. Any updates or significant changes to an Emerging Risk are presented to the Audit & Risk committee. The Audit & Risk Committee and the Board considers Emerging Risks on a regular basis and manages them accordingly, taking into account the expected timing of the risk.

AI Market Product Saturation
Darktrace is a at the forefront of Cyber AI products, as the Group's reputation grows more imitation products will appear using the same core product principles alongside the growth in new generative AI LLMs that competitors are incorporating in their own products which could potentially lead to an over saturation of the market, with cheaper and inferior product lines and the use of new generative AI LLMs trained on inferior data.

AI & Cyber Regulatory uncertainty
Current regulatory trends have prompted companies to re-examine the effectiveness of their governance and oversight. The continued adoption of new or proposed regulations can lead to compliance challenges and to increasing regulatory complexity for Darktrace.

Non-financial information statement and Section 172 (1) statement

The Board considers that it, both as a whole and Stakeholders its individual members, has acted in a way that would be most likely to promote the success of the Group, for the benefit of its members as a whole, whilst having regard to the interests of its other stakeholders in the decisions it has made during the year. The Directors confirm that the meetings and considerations of the Board, which underpin its decisions, incorporate appropriate regard to the matters detailed in section 172 of the Companies Act 2006.

The Board and each Director acknowledges that the success of Darktrace's strategy is reliant on positive engagement with all its stakeholders. The Board believes that Darktrace is stronger and can achieve its goals working in collaboration with, and having regard to, all stakeholders.

Darktrace has a global and diverse community of stakeholders, each with its own interests in and expectations of it. Due to the scale and geographic spread of Darktrace's businesses, stakeholder engagement mostly takes place at an operational level and the Board is therefore reliant on Management to help it fully understand the impact of the Group's operations on its stakeholders.

The Board considers the Group's key stakeholders to be its customers and partners, its people, its shareholders, its suppliers and the communities in which it operates. During the year, the Board considered information from across Darktrace's businesses in the form of reports and presentations from Management and took part in discussions which considered, where relevant, the impact of Darktrace's activities on its key stakeholders. These activities, together with direct engagement by the Board and individual Directors with Darktrace's stakeholders, helped to inform the Board in its decision-making processes.

As a Board, the collective role of the Directors is to act as responsible guardians and stewards of Darktrace. In so doing, the Board ensures that Darktrace is optimally positioned to achieve its long-term sustainable aims and deliver value for its stakeholders. The Board recognises that balancing the needs and expectations of stakeholders is important, but it often must make difficult decisions based on competing priorities where the outcomes are not always positive for all of Darktrace's stakeholders. Decisions are not taken lightly, and the decision-making process has been structured to enable Directors to evaluate proposed business activities and the likely consequences of its decisions over the short, medium, and long term, with the aim of safeguarding Darktrace so that it can continue in existence, fulfilling its purpose and creating value for all stakeholders.

Stakeholders

End-users

Darktrace delivers its cyber AI technology to its customers which defends their most critical digital assets. Whether that business is a multinational corporation with a huge digital footprint or a local business, Darktrace seeks to help them to continue to deliver their products and services to their customers by protecting their digital ecosystem from those who are seeking to exploit it for personal or political gain.

At the heart of Darktrace are its customers and Darktrace remains focussed on bringing more of its cyber AI technology to more organisations around the world. Darktrace customers want products that give them security and peace of mind to focus on what is important to them and their businesses alongside confidence that Darktrace operates efficiently and ethically, keeping its customers' data secure.

People

Darktrace's people are its greatest asset and are critical to the success of the business. Darktrace's people are ambitious: they want to be invested in so that they can succeed in their roles and beyond and they want to play their part in innovating cutting-edge cyber AI technology that plays its part in Darktrace's aim of freeing the world from cyber disruption. Simultaneously, Darktrace's people want to work in an inclusive, ethical environment that they feel connected to and a part of.

As headcount continues to grow, Darktrace has focussed on building and delivering talent development programmes, evolving its internal communications infrastructure to boost engagement and embarking on its Diversity, Equity and Inclusion journey. More information on Darktrace's approach to ESG can be found in the ESG section of Darktrace plc's Annual Report are publicly available: https://ir.darktrace.com/financial-results.

Management has received positive feedback on these efforts through its Influencer Network and more information on this can be found in the ESG section, Investing in People. Darktrace also conducted a company-wide survey in January 2023 to understand employees' needs and to develop strategies to boost culture, engagement and development. Feedback from this survey was strong with a response rate of 74% with an overall score of 7.7 out of 10. The 'relationships' category scored the highest out of all categories, with an average rating of 8.5. Personal growth was identified as an area that employees stated they wanted more of. The launch of the Darktrace Academy is a good first step in this area and the programme will continue to evolve in FY 2024. Darktrace is also evolving its employee surveys to provide richer insights that are tailored to departments and easier for managers to action.

Channel Partners

Darktrace relies on channel partners, including resellers and referral partners, to generate a significant portion of its revenue.

The Partner Programme, the supporting processes and the Partner Team have been enhanced and continue to be improved. This includes the hire of a senior manager to lead the Global Partner Organisation alongside the facilitation of onboarding more high-quality partners and continuously improving its processes and controls around partners.

These enhancements are designed to support Darktrace in making the most of the opportunities provided by the channel community with a view to a faster route to market for Darktrace and, in particular, faster expansion into new markets. In addition the new leader of the Global Partner Organisation and its team will build best-in-class programmes and processes to protect both Darktrace and its customers led by Darktrace's new VP of Partner Programmes & Strategy, who will also lead redesigning the Partner Portal, Deal-registration process and partner enablement programmes.

Suppliers
Darktrace's suppliers support the efficient operation of the business. Suppliers want to receive a fair price and to be paid on time for the products and services they provide.

Darktrace has excellent relationships with its key suppliers and ensures the stability of these relationships by establishing appropriate credit lines that support Darktrace's growth. There are supplier due diligence checks in place, and Darktrace continues to evaluate and, where appropriate, improve controls and processes including in relation to onboarding processes.

Community and broader ecosystem
Darktrace acknowledges that it will only succeed as a business if it uses its technology, expertise and scale to solve the challenges faced by the communities it serves and depends on.

Darktrace understands its core responsibilities to be:

- Data protection and security – empowering society by freeing the world from cyber disruption, particularly small and medium sized businesses ("SMBs");
- Responsible AI innovation;
- Building a diverse technology and cyber workforce; and
- To act as a responsible user of its appropriate share of the world's finite resources.

Management is currently conducting a materiality assessment, comparing external frameworks against community feedback to inform its long term ESG strategy. More information can be found in the ESG section of Darktrace plc's Annual Report are publicly available: https://ir.darktrace.com/financial-results .

Section 172(1) (a) to (f)
A director of a Company must act in the way they consider, in good faith, would be most likely to promote the success of the Company for the benefit of its members as a whole, and in doing so have regard (amongst other matters) to:
a. the likely consequences of any decision in the long term;
b. the interests of the Group's employees;
c. the need to foster the Group's business relationships with suppliers, customers and others;
d. the impact of the Group's operations on the community and the environment;
e. the desirability of the Group maintaining a reputation for high standards of business conduct; and
f. the need to act fairly as between members of the Group.

Non-Financial Information Statement
This section of the report constitutes Darktrace's non-financial information statement, produced to comply with sections 414CA and 414CB of the Companies Act 2006. Refer to Darktrace plc's Annual Report for details : https://ir.darktrace.com/financial-results.

This report was approved by the Board of Directors on 20 November 2023 and signed on its behalf.

DocuSigned by:
Catherine Graham
2AA30F94BFF6408...
Catherine Graham
Director
Date: Nov 21, 2023

Directors' report

The Directors present their report and the financial statements of the Company for the year ended 30 June 2023.

Corporate details
Darktrace Holdings Limited is a company under the UK Companies Act 2006 (the "Act") incorporated in England and Wales under company number 8562035. The principal place of business is Maurice Wilkes Building, St John's Innovation Park, Cowley Road, Cambridge, CB4 0DS.

Information included in the Strategic Report
The strategic report includes a review of the performance of the business (including key performance indicators), principal risks and uncertainties and future developments.

Future development and prospects
Darktrace is in a strong position to leverage the resources it has put in place and the investments it has made in the business during this uncertain economic period. The Executive team, with the support and oversight of the Board, is well placed to take advantage of the business's unique position in the cyber AI market during this pivotal moment for the sector and beyond. Darktrace has long been a global leader in AI and has pioneered a set of products which will protect organisations from the complex and increasingly AI powered threat landscape ahead.

Results and dividends
The audited financial statements of the Company for the period under review are set out on pages 27-56. Darktrace intends to retain any earnings to expand the growth and development of its business and, therefore, does not anticipate paying dividends in the foreseeable future.

Financial Instruments
The Company's financial risk management is controlled by a central treasury department ("Group treasury") under policies approved by the Group's Board. Group treasury identifies and evaluates financial risks in close co-operation with the Company's CFO and other Executive Directors and Senior Managers. The Board authorises written principles for overall risk management, as well as policies covering specific areas, such as foreign exchange risk, interest rate risk, credit risk, use of derivative financial instruments and non-derivative financial instruments, and investment of excess liquidity. In addition, the overall risk framework and strategy for the Company is included within the Strategic Report.

Political Donations
The Company did not make any political donations or incur any political expenditure during the year ended 30 June 2023 and 30 June 2022.

Research and development
The Company has 236 employees working in research and development. Research and development costs increased by $1.4 million to $36.8 million for FY 2023. These are the costs associated with the Company's efforts to develop new products for its platform, expand the features of its platform, and ensure the platform's continuing reliability, availability and scalability. These costs are primarily made up of the labour and related costs remaining after capitalisation of allowable labour and related development costs, and the amortisation of such costs capitalised. Given the Company's rapid growth, for each of the periods presented, the value of costs being capitalised to the statements of financial position have been between two and three times the value of the amortisation of such costs capitalised in prior periods recorded as research and development costs in the statement of comprehensive income. Additionally, research and development does contain allocated overhead costs, primarily rents and other facilities costs that are allocated on a per employee basis.

Employment policies
The Company is committed to following the applicable employment laws in each country in which it operates, adopting fair employment practices and attempts as far as possible to give equal access and fair treatment to all employees. Wherever possible it provides the same opportunities for disabled people as for others. If employees become disabled the Company would make reasonable effort to keep them in employment, with appropriate training where necessary. The Company supports the training needs of its staff including on the job and external training to continue the development of all staff.

Stakeholder and Employee Engagement
Details of the Company's stakeholder and employee engagement is described in the Strategic Report. In addition, Darktrace has established an employee forum as a critical part of its employee engagement and it is through this and a designated NED (Paul Harrison who chairs the Employee Forum) that employees' views can be put forward to the Board.

Gender pay reporting
The Group is required to report its UK gender pay gap annually now that the Group has over 250 employees in the UK. The data below pertains to Darktrace's employees who are based in the UK.

Statutory reportable statistics	**2023**	**2022**
Gender pay gap: mean	4.23%	-1.1%
Gender pay gap: median	14.0%	11.6%
Proportion of men/women in lower quartile pay band (M%/F%)	52.4%/47.6%	56.8%/43.2%
Proportion of men/women in lower middle quartile pay band (M%/F%)	67.5%/32.5%	67.9%/32.1%
Proportion of men/women in upper middle quartile pay band (M%/F%)	78.5%/21.5%	74.2%/25.8%
Proportion of men/women in upper quartile pay band (M%/F%)	64.1%/35.9%	67.9%/32.1%
Proportion of men who received a bonus	80.1%	63.6%
Proportion of women who received a bonus	79.4%	65.7%
Bonus: mean	-43.7%	-42.5%
Bonus: median	34.3%	17.2%

The UK gender gap pay measures the difference between men and women's average pay within an organisation regardless of their role or work level. The gender pay gap is not the same as equal pay, which is related to the law requiring men and women to earn the same salary for the same or a similar job. The mean and median gender pay gap is based on the hourly rate taken at the mandatory snapshot date (April 2023), and includes commission and bonus paid in that month. The mean gender pay data for 2023 shows that the mean pay for women in the UK based workforce is 4.2% lower than for men. The median gender pay data for April 2022 shows that the median pay for men is 14.0% higher than for women.

Darktrace's gender pay results are impacted by the outcomes of bonus and sales commission, which are linked to individual performance. As a consequence, this data tends to fluctuate from month to month. Bonus pay gap is based on the sum of bonus and commission paid within the previous 12 months to April 2023.

The mean bonus gender pay data for 2023 shows that bonuses for women were 43.7% higher than for men. The median bonus gender pay data for 2023 shows that bonuses for men were 34.3% higher than for women. Generally, bonus gap data fluctuates between genders across reporting periods as it is based on individual performance and associated commission paid during that reportable period.

Directors' indemnity arrangements
The Company has maintained Directors' and Officers' liability insurance in respect of its Directors throughout the year.

Going Concern
In adopting the going concern basis for preparing the financial statements, the Directors have considered the Group's principal risks and uncertainties in the current operating environment and assessed these risks via a series of scenario analyses designed to evaluate the capacity of the Group to withstand a prolonged period of adverse financial conditions.

Forecasts and sensitivities have been prepared based on a series of scenarios incorporating plausible yet severe impacts on revenue and ARR, the Group's cost base, and the Group's consolidated statement of financial position including its ability to meet financial covenants.

Throughout, the Directors have considered the viability of the Group's operations with respect to the following fundamental properties of the business:
- a high quality, fast-growth recurring revenue model with high levels of future revenues for which remaining obligations have been fulfilled;
- a variable cost structure which allows the Group to mitigate adverse financial conditions via the flexing of its major cost items; and
- the strong liquidity position of the Group arising from a highly cash-generative model.

The results of these assessments have enabled the Directors to assert a reasonable expectation that the Company has adequate resources to continue as a going concern for a period of at least 12 months from the date of approval of the financial statements. Accordingly, the Directors are of the view that the preparation of the financial statements on a going concern basis continues to be appropriate and in accordance with Financial Reporting Standard 101, 'Reduced Disclosure Framework' (FRS 101) and with the requirements of the Companies Act 2006.

Overseas Branches
Darktrace Holdings Limited has one branch in Dubai which was established in 2019 and one branch in Italy which was established in 2023.

Directors
The Directors who served the Company during the year and at the date of this report, were as follows:
- Ms C Graham
- Mr J Sporle

Financial risk management policies and objectives
For details of the Company's financial risk management policies and objectives please see the Strategic Report.

Environmental matters
As a software company offering virtual installations, Darktrace operates in a relatively low environmental impact sector. However, it is actively looking at ways to minimise its environmental impact and to embed this into every aspect of the company and its operations. Darktrace plc (parent company) reports on global energy consumption and associated GHG emissions in compliance with the Streamlined Energy and Carbon Reporting ("SECR") legislation for listed companies also on behalf of Darktrace Holdings Limited. Please see the Annual Report for Darktrace plc for the year ended 30 June 2023 for further details in this regard.

Post balance sheet events
Details of important events affecting the Company since 30 June 2023 are disclosed in note 26 to the financial statements.

Directors' responsibilities statement
The Directors are responsible for preparing the Strategic Report and Directors' Report and the financial statements in accordance with applicable law and regulations.

Company law requires the directors to prepare financial statements for each financial year. Under that law the Directors have elected to prepare the financial statements in accordance with United Kingdom Generally Accepted Accounting Practice (United Kingdom Accounting Standards and applicable law, including FRS 101 'Reduced Disclosure Framework'). Under company law, the Directors must not approve the financial statements unless they are satisfied that they give a true and fair view of the state of affairs and profit or loss of the Company for that period. In preparing these financial statements, the Directors are required to:

- *select suitable accounting policies and then apply them consistently;*
- make judgements and accounting estimates that are reasonable and prudent;
- state whether applicable UK Accounting Standards have been followed, subject to any material departures disclosed and explained in the financial statements;
- prepare the financial statements on the going concern basis unless it is inappropriate to presume that the Company will continue in business.

The Directors are responsible for keeping adequate accounting records that are sufficient to show and explain the Company's transactions and disclose with reasonable accuracy at any time the financial position of the Company and enable them to ensure that the financial statements comply with the Companies Act 2006. They are also responsible for safeguarding the assets of the Company and hence for taking reasonable steps for the prevention and detection of fraud and other irregularities.

The Directors confirm that:

- so far as each director is aware, there is no relevant audit information of which the Company's auditor is unaware; and
- the directors have taken all the steps that they ought to have taken as Directors in order to make themselves aware of any relevant audit information and to establish that the Company's auditor is aware of that information.

Auditor
The auditor, Grant Thornton UK LLP, will be proposed for reappointment in accordance with section 485 of the Companies Act 2006.

This report was approved by the Board of Directors and signed on its behalf.

DocuSigned by:
Catherine Graham
2AA30F84BFF6408...
Catherine Graham
Director
Date: Nov 21, 2023

Independent auditor's report to the members of Darktrace Holdings Limited

Opinion

We have audited the financial statements of Darktrace Holdings Limited (the 'company') for the year ended 30 June 2023, which comprise the Statement of comprehensive income, the Statement of financial position, the statement in changes in equity and notes to the financial statements, including a summary of significant accounting policies. The financial reporting framework that has been applied in their preparation is applicable law and United Kingdom Accounting Standards, including Financial Reporting Standard 101 'Reduced Disclosure Framework' (United Kingdom Generally Accepted Accounting Practice).

In our opinion, the financial statements:

- give a true and fair view of the state of the company's affairs as at 30 June 2023 and of its profit for the year then ended;
- have been properly prepared in accordance with United Kingdom Generally Accepted Accounting Practice; and
- have been prepared in accordance with the requirements of the Companies Act 2006.

Basis for opinion

We conducted our audit in accordance with International Standards on Auditing (UK) (ISAs (UK)) and applicable law. Our responsibilities under those standards are further described in the 'Auditor's responsibilities for the audit of the financial statements' section of our report. We are independent of the company in accordance with the ethical requirements that are relevant to our audit of the financial statements in the UK, including the FRC's Ethical Standard, and we have fulfilled our other ethical responsibilities in accordance with these requirements. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Conclusions relating to going concern

We are responsible for concluding on the appropriateness of the directors' use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the company's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify the auditor's opinion. Our conclusions are based on the audit evidence obtained up to the date of our report. However, future events or conditions may cause the company to cease to continue as a going concern.

In our evaluation of the directors' conclusions, we considered the inherent risks associated with the company's business model including effects arising from macro-economic uncertainties such as the current global recessionary environment, we assessed and challenged the reasonableness of estimates made by the directors and the related disclosures and analysed how those risks might affect the company's financial resources or ability to continue operations over the going concern period.

In auditing the financial statements, we have concluded that the directors' use of the going concern basis of accounting in the preparation of the financial statements is appropriate.

Based on the work we have performed, we have not identified any material uncertainties relating to events or conditions that, individually or collectively, may cast significant doubt on the company's ability to continue as a going concern for a period of at least twelve months from when the financial statements are authorised for issue.

Our responsibilities and the responsibilities of the directors with respect to going concern are described in the relevant sections of this report.

Other information

The other information comprises the information included in the annual report, other than the financial statements and our auditor's report thereon. The directors are responsible for the other information contained within the annual report. Our opinion on the financial statements does not cover the other information and, except to the extent otherwise explicitly stated in our report, we do not express any form of assurance conclusion thereon.

Our responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with the financial statements or our knowledge obtained in the audit or otherwise appears to be materially misstated. If we identify such material inconsistencies or apparent material misstatements, we are required to determine whether there is a material misstatement in the financial statements themselves. If, based on the work we have performed, we conclude that there is a material misstatement of this other information, we are required to report that fact.

We have nothing to report in this regard.

Opinions on other matters prescribed by the Companies Act 2006

In our opinion, based on the work undertaken in the course of the audit:

- the information given in the strategic report and the directors' report for the financial year for which the financial statements are prepared is consistent with the financial statements; and
- the strategic report and the directors' report have been prepared in accordance with applicable legal requirements.

Matter on which we are required to report under the Companies Act 2006

In the light of the knowledge and understanding of the company and its environment obtained in the course of the audit, we have not identified material misstatements in the strategic report or the directors' report.

Matters on which we are required to report by exception

We have nothing to report in respect of the following matters in relation to which the Companies Act 2006 requires us to report to you if, in our opinion:

- adequate accounting records have not been kept, or returns adequate for our audit have not been received from branches not visited by us; or
- the financial statements are not in agreement with the accounting records and returns; or
- certain disclosures of directors' remuneration specified by law are not made; or
- we have not received all the information and explanations we require for our audit.

Responsibilities of directors

As explained more fully in the directors' responsibilities statement set out on page 21, the directors are responsible for the preparation of the financial statements and for being satisfied that they give a true and fair view, and for such internal control as the directors determine is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, the directors are responsible for assessing the company's ability to continue as a going concern, disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless the directors either intend to liquidate the company or to cease operations, or have no realistic alternative but to do so.

Auditor's responsibilities for the audit of the financial statements

Our objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance but is not a guarantee that an audit conducted in accordance with ISAs (UK) will always detect a material misstatement when it exists.

Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

Irregularities, including fraud, are instances of non-compliance with laws and regulations. The extent to which our procedures are capable of detecting irregularities, including fraud, is detailed below:

- We obtained an understanding of the legal and regulatory frameworks that are applicable to the company through discussions with management. We determined that the most significant frameworks that are directly relevant to specific assertions in the financial statements are those related to the financial reporting framework, being Financial Reporting Standard 101 'Reduced Disclosure Framework' and the Companies Act 2006, together with tax legislation in the jurisdictions in which the company operates, including the application of local sales and use taxes and overseas permanent establishments;
- We enquired of management, the finance team, legal counsel and the board of directors about the company's policies and procedures relating to:
  - the identification, evaluation and compliance with laws and regulations;
  - the detection and response to the risks of fraud; and
  - the establishment of internal controls to mitigate risks related to fraud or non-compliance with laws and regulations.
- We enquired of management and the board of directors whether they were aware of any instances of non-compliance with laws and regulations and whether they had any knowledge of actual, suspected or alleged fraud;
- We assessed matters reported through the company's whistleblowing programme and the results of management's investigations in so far as they related to the financial statements;
- We assessed the susceptibility of the company's financial statements to material misstatement due to fraud, consulting with our forensic specialists to inform this assessment, including how fraud might occur and the risk of management override of controls. Audit procedures performed by the engagement team included:

- Enquiring of management, the finance team, legal counsel and the Board about the risks of fraud at the company, and the controls implemented to address those risks;
- Assessing the design and implementation of controls relevant to the audit that management has in place to prevent and detect fraud, including updating our understanding of the internal controls over journal entries, including those related to the posting of non-standard entries used to record non-recurring, unusual transactions or other non-routine adjustments;
- Making specific inquiries of each member of the finance team to ascertain whether they had been subject to undue pressure or had been asked to make any unusual postings or modifications to reports used in financial reporting;
- Undertaking specific keyword searches (including related parties and previously connected entities and individuals) over the journal entry population to identify descriptions that could indicate fraudulent activity or management override of controls. Journal entries by user were evaluated to identify types of entries posted that were not in line with expectations of their role. Additionally, significant journal entries posted in the year impacting certain KPIs of the company were extracted for testing. All entries noted from these searches were agreed to supporting documentation to corroborate the appropriateness of the posting;
- Performing specific procedures responding to the risk of fraudulent recognition of revenue;
- Challenging assumptions and judgements made by management in its significant accounting estimates;
- Identifying and testing related party transactions; and
- Utilising forensic specialists in our audit testing where we considered it necessary.

- These audit procedures were designed to provide reasonable assurance that the financial statements were free from fraud or error. The risk of not detecting a material misstatement due to fraud is higher than the risk of not detecting one resulting from error and detecting irregularities that result from fraud is inherently more difficult than detecting those that result from error, as fraud may involve collusion, deliberate concealment, forgery or intentional misrepresentations. Also, the further removed non-compliance with laws and regulations is from events and transactions reflected in the financial statements, the less likely we would become aware of it;
- The engagement partner's assessment of the appropriateness of the collective competence and capabilities of the engagement team included consideration of the engagement team's understanding of, and practical experience with, audit engagements of a similar nature and complexity, through appropriate training and participation;
- We communicated relevant laws and regulations and potential fraud risks to all engagement team members, and remained alert to any indications of fraud or non-compliance with laws and regulations throughout the audit.

A further description of our responsibilities for the audit of the financial statements is located on the Financial Reporting Council's website at: www.frc.org.uk/auditorsresponsibilities. This description forms part of our auditor's report.

Use of our report

This report is made solely to the company's members, as a body, in accordance with Chapter 3 of Part 16 of the Companies Act 2006. Our audit work has been undertaken so that we might state to the company's members those matters we are required to state to them in an auditor's report and for no other purpose. To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the company and the company's members as a body, for our audit work, for this report, or for the opinions we have formed.

Grant Thornton UK LLP

Paul Naylor
Senior Statutory Auditor
for and on behalf of Grant Thornton UK LLP
Statutory Auditor, Chartered Accountants
London
Date: Nov 21, 2023

Statement of comprehensive income

	Notes	FY 2023 $'000	FY 2022 $'000
Revenue	5	542,807	414,123
Cost of sales		(57,912)	(45,990)
Gross profit		**484,895**	**368,133**
Sales and marketing costs		(300,564)	(237,160)
Research and development costs		(36,763)	(35,350)
General and administrative costs		(122,750)	(91,336)
Foreign exchange differences		1,698	(3,204)
Other operating income	6	2,666	1,671
Operating profit		**29,182**	**2,754**
Finance costs	7	(4,291)	(2,879)
Finance income	7	3,247	188
Profit for the year before taxation		**28,138**	**63**
Taxation	10	8,931	(2,090)
Net profit/(loss) for the financial year		**37,070**	**(2,027)**
Other comprehensive (loss)/income		-	-
Total comprehensive profit/(loss) for the financial year		**37,070**	**(2,027)**

The notes on pages 31 to 55 are an integral part of these financial statements.

Statement of financial position

	Notes	30 June 2023 $'000	30 June 2022 $'000
Non-current assets			
Intangible assets	11	5,237	6,442
Property, plant and equipment	12	57,799	59,983
Right-of-use assets	13	12,724	18,265
Capitalised commission	14	42,182	32,519
Deposits	16	6,611	7,459
Deferred tax asset	23	10,900	-
Investments	15	64,331	64,252
		199,784	**188,920**
Current assets			
Trade and other receivables	16	126,230	104,322
Capitalised commission	14	34,471	24,635
Tax receivable	10	3,358	2,752
Cash and cash equivalents	17	207,680	157,008
		371,739	**288,716**
Total assets		**571,523**	**477,636**
Current liabilities			
Trade and other payables	18	(97,622)	(105,760)
Provisions	19	(4,856)	(11,842)
Deferred revenue	5	(283,071)	(220,929)
Lease liabilities	13	(873)	(1,153)
		(386,422)	**(339,684)**
Non-current liabilities			
Deferred revenue	5	(28,439)	(29,232)
Lease liabilities	13	(19,402)	(19,402)
Provisions	19	(28)	(2,494)
		(47,869)	**(51,128)**
Total liabilities		**(434,291)**	**(390,812)**
Net assets		**137,232**	**86,825**
Equity			
Share capital	20	100	100
Share premium	20	313,611	313,611
Foreign currency translation reserve		(5,155)	(5,155)
Stock compensation reserve	21	19,238	24,494
Capital contribution	21	66,229	52,878
Retained earnings		(256,791)	(299,103)
Total equity		**137,232**	**86,825**

These financial statements were approved by the Board of Directors and authorised for issue. They were signed on its behalf by:

DocuSigned by:
Catherine Graham
2AA30F94BFF6408...
Catherine Graham
Director
Date: Nov 21, 2023

The notes on pages 31 to 55 are an integral part of these financial statements.

Statement of changes in equity

	Notes	Share capital $'000	Share premium $'000	Foreign currency translation reserve $'000	Stock compensation reserve $'000	Capital contribution $'000	Retained earnings $'000	Total equity $'000
Balance at 30 June 2021		**31**	**313,611**	**(5,155)**	**30,063**	**4,009**	**(302,645)**	**39,914**
Total comprehensive loss for the year:								
Loss for the year		-	-	-	-	-	(2,027)	(2,027)
Other comprehensive loss for the year		-	-	-	-	-	-	-
Total comprehensive loss for the year		**-**	**-**	**-**	**-**		**(2,027)**	**(2,027)**
Preference shares issued	20	69	-	-	-	-	-	69
Capital contribution on acquisition	20	-	-	-	-	15,782	-	15,782
Options exercised	20	-	-	-	(5,569)	-	5,569	-
Capital contribution on account of share-based payments granted by the parent entity	21	-	-	-	-	33,087	-	33,087
Transactions with owners		**69**	**-**	**-**	**(5,569)**	**48,869**	**5,569**	**48,938**
Balance at 30 June 2022		**100**	**313,611**	**(5,155)**	**24,494**	**52,878**	**(299,103)**	**86,825**
Total comprehensive loss for the year:								
Profit for the year		-	-	-	-	-	37,070	37,070
Other comprehensive income/(loss) for the year		-	-	-	-	-	-	-
Total comprehensive profit for the year		**-**	**-**	**-**	**-**		**37,070**	**37,070**
Options exercised	20	-	-	-	(5,256)	(9,695)	5,242	(9,709)
Capital contribution on account of share-based payments granted by the parent entity	21	-	-	-		23,046	-	23,046
Transactions with owners		**-**	**-**	**-**	**(5,256)**	**13,351**	**5,242**	**13,337**
Balance at 30 June 2023		**100**	**313,611**	**(5,155)**	**19,238**	**66,229**	**(256,791)**	**137,232**

The notes on pages 31 to 55 are an integral part of these financial statements.

Notes to the financial statements

1 General information

Company Information
Darktrace Holdings Limited (the Company or Darktrace) is a company incorporated in England and Wales under company number 8562035. The principal place of business is Maurice Wilkes Building, St John's Innovation Park, Cowley Road, Cambridge, CB4 0DS.

2 Basis for preparation

The financial statements of Darktrace Holdings Limited have been prepared in accordance with Financial Reporting Standard 101, 'Reduced Disclosure Framework' (FRS 101). The financial statements have been prepared under the historical cost convention except for certain financial instruments which are measured at fair value, and in accordance with the Companies Act 2006.

The preparation of financial statements in conformity with FRS 101 requires the use of certain critical accounting estimates. It also requires management to exercise its judgement in the process of applying the Company's accounting policies. The areas involving a higher degree of judgement or complexity, or areas where assumptions and estimates are significant to the financial statements, are disclosed in note 3.

The following exemptions from the requirements of IFRS have been applied in the preparation of these financial statements, in accordance with FRS 101:

- Paragraphs 45(b) and 46 to 52 of IFRS 2, 'Share-based payment' (details of the number and weighted average exercise prices of share options, and how the fair value of goods or services received was determined).
- IFRS 7, 'Financial instruments: Disclosures'.
- Paragraphs 91 to 99 of IFRS 13, 'Fair value measurement' (disclosure of valuation techniques and inputs used for fair value measurement of assets and liabilities).
- The following paragraphs of IAS 1, 'Presentation of financial statements':
  - 10(d) (statement of cash flows);
  - 16 (statement of compliance with all IFRS);
  - 38A (requirement for minimum of two primary statements, including cash flow statements);
  - 38B-D (additional comparative information);
  - 111 (statement of cash flows information); and
  - 134-136 (capital management disclosures).
- IAS 7, 'Statement of cash flows'.
- Paragraphs 30 and 31 of IAS 8, 'Accounting policies, changes in accounting estimates and errors' (requirement for the disclosure of information when an entity has not applied a new IFRS that has been issued but is not yet effective).
- Paragraph 17 of IAS 24, 'Related party disclosures' (key management compensation).
- The requirements in IAS 24, 'Related party disclosures', to disclose related party transactions entered into between two or more members of a group.

All amounts in the financial statements and notes have been rounded to the nearest thousand USD, unless otherwise stated.

New Standards, Amendments, IFRIC Interpretations and new Relevant Disclosure Requirements Adopted by the Company
There are no amendments to accounting standards, or IFRIC interpretations that are effective for the period ended 30 June 2023 that have a material impact on the Company's financial statements.

New standards and interpretations not yet adopted
Certain new accounting standards, amendments to accounting standards and interpretations have been published that are not mandatory for 30 June 2023 reporting periods and have not been early adopted by the group. These standards, amendments or interpretations are not expected to have a material impact on the entity in the current or future reporting periods an on foreseeable future transactions.

Consolidation

The Company is a wholly owned subsidiary of Darktrace plc. It is included in the consolidated financial statements of Darktrace plc, which are publicly available. Therefore, the Company is exempt, by virtue of section 400 of the Companies Act 2006, from the requirement to prepare consolidated financial statements. The address of the ultimate parent's registered office is Maurice Wilkes Building, St John's Innovation Park, Cowley Road, Cambridge, United Kingdom, CB4 0DS.

These financial statements are separate financial statements.

Going Concern

In adopting the going concern basis for preparing the financial statements, the Directors have considered Darktrace's principal risks and uncertainties in the current operating environment and assessed these risks via a series of scenario analyses designed to evaluate the capacity of Darktrace to withstand a prolonged period of adverse financial conditions. The Directors have further reviewed liquidity and covenant forecasts for the period to 30 November 2024 as part of their assessment of going concern.

The Directors have considered how a change in circumstances might impact Darktrace's expected financial performance for the period. Specifically, testing has been performed on the base case forecast for the period and a number of adverse scenarios have been modelled, including but not limited to:

- Annualised Recurring Revenue (ARR)/revenue scenarios: The impact of material reputational damage on new customer acquisition and existing customer churn arising as a result of a data breach or cyber incident, combined with significant operational disruption and declines in salesforce productivity, as a result of a service provision downtime or a lack of future product innovation. Each of the scenarios would materially reduce Darktrace's ARR and revenue, and it was assumed, for example that there would be zero new logo ARR across the entire period along with a material deterioration in net ARR retention trends. No active cost saving measures were implemented during the period.
- Cost scenarios: Either as a result of increased industry competition and/or reputational damage, the impact of a material and prolonged failure in Darktrace's ability to attract and retain employees was considered, leading to significant increases in employee churn and hiring and compensation related costs. For example, expected employee churn rates for the entire salesforce and the remaining wider workforce were increased by 25% and 20% respectively. Meanwhile hiring and compensation costs were materially increased, particularly for technical and sales-related personnel, and extended general cost inflation was considered, with material increases to key unit costs (such as appliance and hosting costs). No active cost saving measures were implemented during the period.
- Balance sheet scenarios: Either as a result of a significant macroeconomic event with recessionary impact and/or inadequate channel partner management and support, the impact of changes to direct and indirect customer payment terms and increased customer insolvencies was considered. For example, forecast collection rates were modelled to drop lower than at any point during the worst of the COVID-19 uncertainty and corresponding payment delays. Meanwhile estimated bad debt expense for the period was increased fivefold vs. the base case forecast, and the Group's base case forecast invoicing profile was amended to include a material shift towards quarterly and monthly invoicing.
- Combined, 'worst case' scenario: This scenario sought to present an extreme and unreasonable 'worst case' outcome by combining the three aforementioned scenarios. No active cost saving measures were enacted during the period and the Group remained viable and in compliance with its covenants within the period.

In each variation and combination of the adverse scenarios, Darktrace is forecast to have sufficient resources to continue to meet its liabilities as they fall due for at least 12 months from the date of approval of the financial statements, and for each scenario, active cost saving actions were not instigated as part of the analysis. In the event that any of these adverse scenarios were to occur, controllable mitigating actions are available to the Directors should they be required.

As an additional provision, the Directors also reviewed the results of reverse stress testing performed to provide an illustration of the level of churn and deterioration in new customer acquisition and customer payment terms which would be required to trigger a breach in Darktrace's covenants or exhaust cash down to minimum working capital requirements. The conditions necessary to approach either of these parameters are extreme and would ultimately require no active cost saving actions to be enacted at any point. As such, the Directors consider their likelihood as highly remote given the resilient nature of the business model, as demonstrated by the growth in revenues, customer numbers and employees in recent reporting periods. The robust consolidated statement of financial position, with $207.7 million of cash available and continued strong receivables collection rate of the Group demonstrated during the COVID-19 pandemic and the macroeconomic uncertainties through FY 2023 gives further support to the resilience of Darktrace's business model.

The results of these assessments have enabled the Directors to assert a reasonable expectation that Darktrace has adequate resources to continue as a going concern for a period of at least 12 months from the date of approval of the financial statements. Accordingly, the Directors are of the view that the preparation of the financial statements on a going concern basis continues to be appropriate and in accordance with FRS 101 and with the requirements of the Companies Act 2006.

Foreign currency translation

Functional and presentation currency

Items included in these financial statements are measured using the functional currency for the Company. The financial statements are presented in U.S. Dollars ("USD") which, since 1 July 2019, has been the functional currency of the Company.

Transactions and balances

Foreign currency transactions are translated into the functional currency of the Company using the exchange rate as at the time of transaction. Foreign exchange gains and losses resulting from the settlement of such transactions, and from the translation of monetary assets and liabilities denominated in foreign currencies at month end exchange rates, are generally recognised in the statement of comprehensive income. All other foreign exchange gains and losses are presented in the statement of comprehensive income on a net basis within other gains or losses. Translation differences on assets and liabilities carried at fair value are reported as part of the fair value gain or loss.

Impairment of non-financial assets

Assets are tested for impairment whenever events or changes in circumstances indicate that the carrying amount may not be recoverable. Intangible assets that are not subject to amortisation because they are not yet in use are tested annually for impairment, or more frequently if events or changes in circumstances indicate that they might be impaired. An impairment loss is recognised for the amount by which the asset's carrying amount exceeds its recoverable amount. The recoverable amount is the higher of an asset's fair value less costs of disposal and value in use. For the purposes of assessing impairment, assets are grouped at the lowest levels for which there are separately identifiable cash inflows which are largely independent of the cash inflows from other assets or groups of assets (cash-generating units). Non-financial assets that suffered an impairment are reviewed for possible reversal of the impairment at the end of each reporting period. Reversals of impairment losses are limited such that the value of the asset cannot exceed the carrying amount it would have had no impairment been recognised.

3 Key judgements and estimates

The preparation of financial statements in accordance with FRS 101 requires Management to make judgements, estimates and assumptions that affect the reported amount of assets and liabilities and disclosure of contingent assets and liabilities at the period end and the reported amount of revenues and expenses during the reported period. Actual results may differ from these estimates. Estimates and underlying assumptions are reviewed on an ongoing basis. Revisions to accounting estimates are recognised in the period in which the estimates are revised and for any future periods affected.

The areas involving significant judgements and estimates are:

- Significant judgement in revenue recognition in determining one performance obligation exists – see note 5
- Significant judgement in assessment of control of appliances – see note 12
- Significant judgement and estimate in deferred tax asset (DTA) recognised on UK losses carried forward– see note 23
- Significant estimate in share price used to calculate the provision for share option related employer tax changes – see note 19.

4 Operating segment

Segment reporting

The Company has concluded that it operates in one business segment as defined by IFRS 8: Operating Segments, being the development and sale of cyber-threat defence technology. The Chief Operating Decision Makers (the "CODMs"), which have been identified as the Chief Executive Officer (CEO) and Chief Financial Officer (CFO), make operating decisions for a single operating unit and operating performance is assessed as a single operating segment. The information used by the CODMs includes the information presented in these financial statements, as well as various alternative performance measures as disclosed in these financial statements. Further there are no separately identifiable assets attributable to any separate business activity or business unit.

Non-current assets by geographical market

	30 June 2023 $'000	30 June 2022 $'000
United Kingdom	38,584	45,310
USA	34,739	33,755
Europe	81,419	75,788
Rest of World	27,531	26,608
	182,273	**181,461**

5 Revenue from contracts with customers

Revenue recognition policy

The Company does not recognise any revenue until there is a legally binding contract in place with a customer or reseller partner acting on behalf of a customer (i.e. end-user), the commencement date of that agreement has passed, and the obligations to fulfil that contract have been met. It applies the IFRS 15: Revenue from Contracts with Customers, principles-based, five step model to all contracts as follows:

- Identify the contract with the customer,
- Identify the distinct performance obligations in the contract,
- Determine the transaction price,
- Allocate the transaction price to the performance obligations in the contracts, on a relative stand-alone selling price basis, and
- Recognise revenue when the entity satisfies its performance obligations.

The Company has only a single performance obligation for most contracts, giving access to the Company's Cyber AI Platform and ancillary services to its customers as such the transaction price is the total amount charged to the customer over the service period.

Most of the Company's revenue is derived from multi-period subscription or licence contracts that allow access to the Cyber AI Platform. This revenue is recognised on a straight-line basis over the subscription or licence period as the customer simultaneously receives and consumes the benefits from the products it purchased within the Company's Cyber AI Platform as throughout the life of the contract. The Company's efforts are expended evenly throughout the subscription period and therefore using the input method under IFRS 15, it is appropriate to recognise revenue on a straight-line basis. The Company does not have any variable consideration as defined under IFRS 15.

In a very small number of cases, the Company sells supplementary training or extra appliances separately from its software product deployments, but always to customers who have software product deployments. The revenue from these contracts is recognised at the point in time when the training or appliance is delivered.

Contracts where terms are subsequently modified (for upsells, license expansions, etc) are assessed in accordance with IFRS 15 and are treated either as a separate contract with revenue recognition commencing from the modification date or as a cumulative catch-up adjustment to revenue recognised at the point of modification based on the new contractual terms.

Contracts where it is not probable that the Company will collect the consideration to which it will be entitled in exchange for the goods or services that will be transferred to the customer and for which a suspension notice has been applied and the performance obligations relating to future services is considered curtailed, are considered ceased and therefore related deferred revenue balances are derecognised and any receivable balance fully provided or written off. In this case, Management accounts for the remainder of the contract as if the criteria to be a contract had not been met (IFRS 15).

The Company deploys a significant portion of its software on appliances that it delivers to the customer. These appliances are encrypted devices that can only be used to run the Company's software. They cannot be used for any other purpose and have no separate value to the customer, and as the Company retrieves its appliances at the end of deployments, each appliance may be redeployed multiple times, in multiple situations over its useful life. The Company considers that the appliances it deploys are an integral part of the delivery mechanism for the service to the customer and are not normally sold to the customer unless required for legal or regulatory reasons.

Customers are generally billed in advance, with credit terms of typically 30-60 days, in line with market practice. In instances where payment for the subscription is within 12 months or less of the service being provided Darktrace has taken the practical expedient under the standard of not adjusting for any financing component. In some instances, the Company bills in advance for periods of greater than one year. In these instances no financing component is deemed to be present as this arrangement is customer driven.

Principal versus agent assessment
Darktrace sells its products and services either directly to end-users or through channel partners. The business operates two types of partner relationships, one where the contract is with the reseller partner and another where it is with the end-user but the partner receives a referral fee.

Most partner deals involve a reseller partner who takes Darktrace to the end-users. In these instances, Darktrace sells to the reseller partner, who is the contracting entity, and therefore different from the end-user that will be provided with the services. Darktrace will only invoice the partner and it is the partner who controls pricing with the end-user, and bears the credit and foreign currency risk.

When revenues are generated through a reseller partner, Darktrace requires that every partner contract be related to a specific end-user (Darktrace has a direct operating relationship with the end-user as most partner contracts are co-sold and Darktrace employees carry out the vast majority of pre-sale product scoping directly with the end-user). Darktrace only recognises revenue for the contract value between Darktrace and the partner, it does not recognise any benefit from any mark-up that the partner adds to determine its price to the end-user. Once the Darktrace/partner and partner/end-user contracts have been finalised and the end-user is able to deploy the purchased products and services, Darktrace will recognise revenue as required under IFRS 15.

An intermediary partner is the principal in an arrangement with the end-user, and therefore, Darktrace's customer, if it controls the offering before it is transferred to the end-user. As Darktrace controls all aspects of the products and services it sells, including setting the price to the reseller partner (but not the end-user), and bears the credit and foreign exchange risk in its contract with the reseller partner, it has concluded that Darktrace is a principal in its contracts with reseller partners. Darktrace has also considered the role of the reseller partner in their contract with the end-user, and based on all information available, primarily considering the control of pricing and the assumption of credit and foreign exchange risk, has concluded that the reseller is principal in their contract with the end-user. While Darktrace has responsibility under its Master Service Agreement for fulfilment of the products and services provided to the end-user, the reseller partner has responsibility for the pricing of Darktrace products to the end-user, and any invoicing and credit concerns.

There is a smaller cohort of referral partners who Darktrace works with who will initiate the customer contact, but who do not take on the contractual risk. In these cases, Darktrace enters into a direct contract with the end-user and is therefore the principal in these transactions. The partner will earn usually a commission or a fee which is classified as sales and marketing cost.

Significant Judgement in Revenue Recognition in Determining one Performance Obligation Exists
Company revenue is from subscription contracts and is recognised over the term of the contract.

Management considers that these contracts consist of a single performance obligation, which is the ongoing access to the portions of the Cyber AI platform purchased by the customer. The Cyber AI platform is a single combined solution, with customers able to choose the appropriate product mix based on their own needs. The key contractual elements considered by Management included the deployment of the software (on appliances or virtually), the core software products and subsequent updates. Appliance deployments typically take an hour or less once the appliance is received by the customer, and virtual deployments can be enabled immediately, so deployment is not a material performance component of a subscription contract that has, on average, a three-year life. Subsequent updates to the platform ensure that the latest software is available with the latest capabilities but do not materially change the functionality of the platform. The products and, to a lesser extent, services are significantly integrated to provide a combined output and services which are highly interdependent with (and are not separately available from) the subscription to product within the Cyber AI platform. Some customers may purchase ancillary services or training, but these are immaterial to the total contract value and are not deemed to impact the assessment of there being only a single performance obligation.

Disaggregation of revenue
Revenue recognised at a point in time is not significant to the reported results in any year. This includes revenue generated by separate contracts for training and sale of appliances. In the year ended 30 June 2023 this revenue amounted to $0.3 million (30 June 2022: $1.5 million).

Management has assessed that the single performance obligation that it is providing to customers is access to products, primarily software, within the Darktrace Cyber AI platform to protect customers' digital estates from the impact of cyber threats.

	FY 2023 $'000	%	FY 2022 $'000	%
USA	188,791	34.8%	142,696	34.5%
United Kingdom	82,841	15.3%	69,228	16.7%
Europe	133,060	24.5%	98,886	23.9%
Rest of World	138,115	25.4%	103,313	24.9%
	542,807	100%	**414,123**	100%

Revenue from customers has been attributed to the geographic market based on contractual location. No single customer accounted for more than 10% of revenue in FY 2023 or FY 2022.

Contract assets and liabilities related to contracts with customers
The following table provides information on accrued income and deferred revenue from contracts with customers.

	30 June 2023 $'000	30 June 2022 $'000
Accrued income	3,445	4,152
Total accrued income	**3,445**	**4,152**
Current deferred revenue	283,071	220,929
Non-current deferred revenue	28,439	29,232
Total deferred revenue	**311,510**	**250,161**

Deferred revenue has increased year on year in line with the increase in revenue.

Contracts are invoiced between one month and more than three years in advance, with the majority of contracts being invoiced annually in advance. Deferred revenue reflects the difference between invoicing and associated payment terms, and fulfilment of the performance obligation.

Details of costs to obtain contracts with customers are shown in note 14.

Revenue recognised in relation to deferred revenues (contract liabilities)
The following table shows how much revenue recognised in each reporting year related to brought-forward contract liabilities:

Revenue recognised in relation to contract liabilities	FY 2023 $'000	FY 2022 $'000
Revenue recognised that was included in the contract liability balance at the beginning of the period	220,929	154,505

Future contracted revenue (formerly revenue expected to be recognised)
Future contracted revenue represents revenue expected to be recognised over the term of the contract, i.e. over the subscription period, from the contract commencement date to the end of the subscription period as identified in the contract, calculated by valuing all uninvoiced future contract value, including one-time product or service purchases, at the exchange rates in effect on the reporting date, and all previously invoiced future revenue at the relevant transaction exchange rates. In line with IFRIC 22, the date of the transaction for the purpose of determining the exchange rate to use on initial recognition of the related asset, expense or income (in whole or part) is the date on which an entity initially recognises the non-monetary asset or non-monetary liability arising from the payment or receipt of advance consideration. One-time revenue is included in the calculation but because of the high proportion of subscription revenue in Darktrace's revenue base, it is not material. Future contract value does not include any opt-out clauses i.e. revenue expected after opt-out date, up to the termination date of the contract.

Prior year adjustment to the disclosure
However, subsequent to the publication of its FY 2022 Annual Report, Darktrace identified that "Revenue expected to be recognised" i.e. future contracted revenue mistakenly included expected revenue after the opt-out date, inconsistent with IFRS 15 paragraph 11. This error accounts for $33.3 million mistakenly disclosed in the expected future revenue to be recognised. Darktrace has corrected the error in its disclosure in these financial statements as presented below. This did not affect any reported numbers in the primary financial statements and the error was limited to this disclosure only.

	FY 2022 Before restatement $'000	Restatement $'000	FY 2022 Restated $'000
Due within 12 months	475,535	(25,594)	449,941
Due within 1-2 years	329,888	(4,335)	325,553
Due within 2-3 years	196,532	(1,833)	194,699
Due within 3-4 years	60,793	(433)	60,360
Due over 4 years	4,621	(41)	4,580
	1,067,369	**(32,237)**	**1,035,132**

	FY 2023 $'000	FY 2022 Restated $'000
Due within 12 months	575,775	449,941
Due within 1-2 years	397,758	325,553
Due within 2-3 years	216,494	194,699
Due within 3-4 years	72,263	60,360
Due over 4 years	3,552	4,580
	1,265,843	**1,035,132**

6 Other operating income

R&D tax credit / Government grants

The Company has made claims for tax credits under the HMRC RDEC scheme since 2019 which is reflected as other income on the consolidated statement of income. This accounting treatment is in accordance with IAS 20 Government grants.

	FY 2023 $'000	FY 2022 $'000
R&D tax credit under HMRC RDEC scheme	2,666	1,671

7 Finance costs and finance income

Finance income and costs

The Company earns interest on its cash balances through its deposits with banks.

Interest income on financial assets at amortised cost is calculated using the effective interest method and is recognised in the statement of comprehensive income as part of other income.

All finance costs are recognised in the statement of comprehensive income as part of finance costs in the period in which they are incurred.

	FY 2023 $'000	FY 2022 $'000
Finance costs		
Interest on lease liabilities	4,291	2,879
Total Finance costs	**4,291**	**2,879**
Finance income		
Interest income from cash and cash equivalents	3,247	188
Total Finance income	**3,247**	**188**

8 Material profit or loss items

Cost of sales

Cost of sales is made up of two primary cost categories: the cost of software deployment and labour costs for support or supplemental monitoring and response services.

The largest of the deployment costs is depreciation on appliances used to deliver the software to customers under contracts. The depreciation of appliances is apportioned to Cost of sales based on the proportion of the Company's appliance pool deployed to customer sites and all appliance depreciation related to customer contracts is recognised in Cost of sales. Where the Company deploys software to a contracted customer virtually, the associated hosting costs are also recognised in Cost of sales. Cost of sales also includes shipping costs and other costs necessary to deploy the Company's software products.

Operating cost apportionment
Wherever possible, operating costs are attributed to either sales and marketing, research and development or other administrative costs by the direct method. When costs apply to more than one cost category, they are apportioned using an allocation methodology based on the most appropriate direct data source.

The Company apportions the depreciation of appliances used to run Proof of Value ("POV") demonstrations for prospects (see note 12 for additional detail) to sales and marketing. Similarly, for POVs of virtually deployed products, the associated hosting costs are recognised as sales and marketing costs. Also, pre-sales support staff, whose costs are primarily attributed to Sales and marketing, may also perform post-sales support functions. This work is tracked, and the compensation costs associated with that work are allocated to Cost of sales.

Research and development ("R&D") primarily consists of compensation and other directly attributable costs of the staff who develop the Company's software products. The Company capitalises the costs of development work that meets the criteria for capitalisation and amortises those costs beginning once the software is released to production and/or brought into use. Developers and Analysts working in the Company's R&D function may also provide supplemental monitoring and response services to customers. This work is tracked and the compensation costs associated with that work are allocated to Cost of sales. Research and development expenditures that do not meet the criteria for capitalisation, are recognised as expense when incurred. Development costs previously recognised as expenses are not recognised as assets in any subsequent period. Development costs for features and enhancements that are available to all customers without additional charge, are expensed as incurred.

Share-based payment cost and related share-option employer tax charges are apportioned on a direct basis depending on the department the employee reports into.

The Company has identified a number of items which are material due to the significance of their nature and or amount. These are listed separately here to provide a better understanding of the financial performance of the Company, if not presented elsewhere in these financial statements.

	FY 2023 $'000	FY 2022 $'000
Hosting fees	21,353	15,191
Legal and professional fees	6,670	5,912
New software implementation costs	3,873	-
Auditors' remuneration	684	532
Brand strategy costs	-	2,030

Hosting fees related to customer contracts are classified within cost of sales for an amount of $16.9 million (FY 2022 $10.7 million) and those related to POV are classified to sales and marketing costs for an amount of $4.5 million (FY 2022 $4.5 million).

Legal and professional fees increased as a result of increased corporate activities, the refinancing activity and some legacy litigation cost.

Brand strategy costs in the prior year related to costs for Darktrace's new branding and logo change.

Auditors' remuneration includes the audit fees of the Company accounts.

9 Employee costs

Employees benefits
Short-term obligations
Liabilities for wages and salaries, including non-monetary benefits, annual leave and accumulating sick leave that are expected to be settled wholly within 12 months after the end of the period in which the employees render the related service are recognised up to the end of the reporting period and are measured at the amounts expected to be paid when the liabilities are settled. The liabilities are presented as current employee benefit obligations in the statement of financial position.

Post-employment obligations - Defined contribution plans
For defined contribution plans, the Company pays contributions to publicly or privately administered pension insurance plans on a mandatory, contractual or voluntary basis. The Company has no further payment obligations once the contributions have been paid. The contributions are recognised as employee benefit expense when they are due. Prepaid contributions are recognised as an asset to the extent that a cash refund or a reduction in the future payments is available.

The Company operates a stakeholder pension scheme and contributes to several personal pension schemes on behalf of its employees. The Company also contributes to State-sponsored pension schemes in multiple countries as legislated.

Bonus plans
The Company recognises a liability and an expense for bonuses based on management's best estimate of the expected payment for discretionary bonuses and then will make the appropriate adjustments if necessary, at the time these bonuses are paid. The Company recognises a liability where contractually obliged or where there is a past practice that has created a *constructive obligation.*

Employee benefits expense
Expenses recognised for the Company's employee compensation and benefits is presented below:

	FY 2023 $'000	FY 2022* $'000
Wages and salaries	117,117	93,757
Social security	12,910	11,221
Pension	1,989	1,696
Employee cost	**132,016**	**106,674**
Share based payment charge	22,340	31,600
Total cost	**154,356**	**138,274**

Total cost is split as follows:

	FY 2023 $'000	FY 2022* $'000
Cost of sales	7,586	6,165
Sales and marketing	93,072	87,117
Research and development	16,166	18,972
Other administrative	37,532	26,020
Total cost	**154,356**	**138,274**

*Prior year wages and salaries figure was incorrectly disclosed net of $19.1 million being the capitalised commission cost net of the related amortisation.

The average number of employees, including Executive Directors, during the year was as follows:

	FY 2023 Number	FY 2022 Number
Sales and marketing	532	443
Research and development	238	200
Administration and operations	257	220
	1,027	**863**

Directors' emoluments and benefits were as follows:

	FY 2023 $'000	FY 2022 $'000
Emoluments	1,495	1,725
Gains on exercise of share options	8,934	1,760
	10,429	**3,485**

Total amounts payable to the highest paid director were $940,348 (2022: $1,252,083) in respect of emoluments. Two Directors were members of the Company's defined contribution pension schemes in 2023 and 2022.

10 Tax expense

Income tax

The income tax expense or credit for the period comprises current tax for the year, based on the applicable income tax rate for each jurisdiction, adjusted by changes in deferred tax assets and liabilities attributable to temporary differences and to unused tax losses, where applicable.

Current tax is the expected tax payable or receivable on the taxable income for the year, using tax rates enacted or substantively enacted at the end of the reporting period, and any adjustment to tax payable in respect of previous periods in the countries where the Company operates and generates taxable income. Any uncertain tax treatments are reviewed, documented and communicated to the Company's Board as appropriate. The Company finance function monitors any uncertain items on a regular basis, working closely with the local tax advisor to understand any potential changes to the associated risk. The amount of current tax payable or receivable is the best estimate of the tax amount expected to be paid or received that reflects uncertainty related to income taxes.

Deferred tax assets are recognised only if it is probable that future taxable amounts will be available to utilise those temporary differences and losses.

Deferred tax assets and liabilities are offset where there is a legally enforceable right to offset current tax assets and liabilities and where the deferred tax balances relate to the same taxation authority. Current tax assets and tax liabilities are offset where the Company has a legally enforceable right to offset and intends either to settle on a net basis, or to realise the asset and settle the liability simultaneously.

Deferred income tax is determined using tax rates (and laws) that have been enacted or substantively enacted by the end of the reporting period and are expected to apply when the related deferred income tax asset is realised, or the deferred income tax liability is settled.

Income tax is recognised as an expense or income and included in the statement of comprehensive income for the period, except to the extent that the tax arises from a transaction or event that is not itself recognised in the statement of comprehensive income, for example when it relates to items recognised in other comprehensive income or directly in equity. In this case, the tax is also recognised in other comprehensive income or directly in equity, respectively.

Significant judgement and estimate in deferred tax asset (DTA) recognised on losses carried forward

At 30 June 2023 the Company has significant tax losses in the UK available for offset against future taxable profits. The Group has recognised a DTA on UK losses carried forward of approximately $10.9 million (30 June 2022: nil) and an unrecognised DTA on UK losses carried forward of approximately $50.2 million (30 June 2022: $51.7 million) as Management believes there is insufficient convincing other evidence that the potential asset will be utilised in the foreseeable future, which is required for recognition under IAS 12 when there is a history of losses.

<u>Significant judgement</u>

When assessing if it is probable that future taxable profits will be available, given the long history of tax losses, Management has determined whether sufficient positive evidence outweighs existing negative evidence. The longer the estimates or forecasts extend into the future, the less reliable they are. Management believes the most appropriate period to be used in order to make the assessment on the future taxable profit and the recoverable deferred tax asset on UK losses carried forward is two years. In particular, whilst from a cash flow perspective given the strong cash position, a three-year period for a viability analysis is considered appropriate, the profitability is sensitive to changes that depend much more on the current and future macro-economic environment, inflation and foreign exchange trends. Had a three-year period been considered, a further $6.3 million UK deferred tax asset on losses carried forward would have been recognised at 30 June 2023.

<u>Significant estimate</u>

The estimates or forecasts used for the determination of the future taxable profits for the UK entity used consistent assumptions to those used elsewhere. Currently there is sufficient convincing other evidence on the certainty of sufficient future taxable profits in the UK over the next two years, which will enable Darktrace Holdings Limited to start utilising its brought forward tax losses, therefore an initial recognition of the deferred tax asset in relation to losses carried forward has been done in the year for an amount of $10.9 million

The estimates take account of the inherent uncertainties constraining the expected level of profit as appropriate, however part 12 deductions have not been taken into account given the uncertainty of the tax deduction in excess of IFRS2 change recognised for share-based payments. Possible changes in the estimates made, will affect future profits and therefore the recoverability of the deferred tax assets. An increase in operating costs by 10% would bring the UK entity into tax loss position over the next two years and therefore no DTA ($10.9 million) on UK losses carried forward should be recognised. In contrast, a decrease in operating costs by 10% would bring a significant increase in the tax profit for the UK entity increasing the recognisable DTA by $16.5 million.

	FY 2023 $'000	FY 2022 $'000
Current tax		
Current tax	794	1,336
Adjustments in respect of prior periods	1,175	754
Total current tax	**1,969**	**2,090**
Deferred tax		
Recognition of deferred tax asset on losses carried forward	(10,900)	-
Total deferred tax	**(10,900)**	**-**
Tax (credit)/charge for the period	**(8,931)**	**2,090**

The relationship between the expected tax expense based on the UK effective tax rate of the Company at 20.5% (2022: 19.0%), and the tax expense recognised in the statement of comprehensive income can be reconciled as follows:

Reconciliation of tax charge	FY 2023 $'000	FY 2022 $'000
Profit on ordinary activities before tax	28,138	63
Tax reconciliation:		
Tax on profit on ordinary activities at standard CT rate 20.5% (FY22 - 19.0%)	5,768	12
Effects of:		
Non-deductible expenses	3,580	6,730
Overseas taxes deducted at source	607	817
Tax cost on research and development tax credit	560	186
Under provided in prior years	1,175	754
Current tax exchange differences arising on movement between opening and	-	112
Fixed Asset Differences - Super deduction net of Ineligible depreciation and	(1,202)	(1,687)
Unrecognised deferred tax current year movement	(6,455)	(4,834)
Deferred tax recognised	(12,965)	-
Tax (credit)/charge for the period	**(8,931)**	**2,090**

The tax charge in the current and prior years primarily relates to overseas tax.

11 Intangible assets

Intangible assets

The Company capitalises allowable costs related to the development of new products and related significant functional enhancements to its Cyber AI platform. The directly attributable costs capitalised are employee costs including the appropriate portion of relevant compensation-related overheads. Costs are only capitalised when the following criteria are met:

- it is technically feasible to complete the software so that it will be available for use,
- management intends to complete the software so that it will be available for use,
- there is an ability to use or sell the software,
- it can be demonstrated how the software will generate probable future economic benefits,
- adequate technical, financial and other resources to complete the development and to use or sell the software are available, and
- the expenditure attributable to the software during its development can be reliably measured.

These capitalised development costs are recorded as intangible assets and amortised from the point at which the developed assets are released for use, typically as a part of major version or product releases.

Capitalised development costs are amortised on a straight-line basis over a three-year period unless the related software is removed from service prior to that date, in which case the remaining amortisation related to the software removed from use would be accelerated. Amortisation is classified as research and development costs.

Costs associated with maintaining software programmes are recognised as an expense as incurred.

Software consists of capitalised development costs being internally generated intangible asset of $2.3 million (30 June 2022: $4.9 million). The Group has not identified any impairments to the intangibles. All amortisation of intangible assets is charged to the statement of comprehensive income and is included within research and development costs.

	30 June 2023			30 June 2022		
	Software $'000	Software under development $'000	Total $'000	Software $'000	Software under development $'000	Total $'000
Cost:						
As at 1 July	16,528	1,517	18,045	13,286	-	13,286
Additions	-	2,519	2,519	2,391	2,368	4,759
Reclassification	1,082	(1,082)	-	851	(851)	-
Foreign exchange difference						
At 30 June	**17,610**	**2,954**	**20,564**	**16,528**	**1,517**	**18,045**
Amortisation:						
As at 1 July	(11,603)	-	(11,603)	(6,199)	-	(6,199)
Charge for the year	(3,724)	-	(3,724)	(5,404)	-	(5,404)
At 30 June	**(15,327)**	**-**	**(15,327)**	**(11,603)**	**-**	**(11,603)**
Net book value	**2,283**	**2,954**	**5,237**	**4,925**	**1,517**	**6,442**

12 Property, plant and equipment

Property, plant and equipment is stated at historical cost less depreciation. Historical cost includes expenditure that is directly attributable to the acquisition of the items. Subsequent costs are included in the asset's carrying amount or recognised as a separate asset, as appropriate, only when it is probable that future economic benefits associated with the item will flow to the Company and the cost of the item can be measured reliably. The carrying amount of any component accounted for as a separate asset is derecognised when replaced. All other repairs and maintenance are charged to the statement of comprehensive income during the reporting period in which they are incurred.

The depreciation methods and periods used by the Company are as follows:

Appliances	5 years straight line
Leasehold improvements	Lower between UEL and lease term on straight line
Equipment	2-5 years straight line

The assets' residual values and useful lives are reviewed, and adjusted if appropriate, at the end of each reporting period. Gains and losses on disposals are determined by comparing proceeds with carrying amount. These are included in the statement of comprehensive income. For more details around the critical judgement and significant estimates around appliances see below.

Other assets

Other assets included within property, plant and equipment are generally IT equipment for employee use and a small amount of infrastructure equipment. The Company also has office fit out costs, furniture, other tangible property including leasehold improvements.

Appliances

Most of the Company's property, plant and equipment is comprised of the appliances used to deploy its software. Appliances are encrypted with the Group's software and deployed both to customers for the fulfilment of contracts and potential customers for POV demonstrations. These appliances are deployed, retrieved and redeployed many times over their useful lives and may be on customer or prospect sites, interchangeably, at any given time. The Group retains ownership of these appliances and depreciates them over an estimated five-year useful economic life. The depreciation of these assets is apportioned to either Cost of sales or Sales and marketing based on the proportion of appliances deployed to customers and prospects in each period.

Significant judgement in assessment of control of appliances

The Company is required to assess if, as part of the assessment of the performance obligations, there is an embedded lease within the contract relating to the appliances used to deploy its software. Due to the length of the contracts, averaging approximately three years, and the underlying asset value, it is appropriate to assess if there is an inherent lease embedded within the contract.

The Company considered its continued ownership of the appliances, the appliances having a useful economic life in excess of the typical contract length (appliances are accounted for on an estimated useful life of five years based on the Company's experience to date), and the appliances being an immaterial portion of the total contract value in determining if there was a lease. It is Management's judgement that the Company retains control of the appliances throughout the performance period as the Company directs the use of the asset. It is also Management's judgement that the Company's contracts do not contain leases under IFRS 16.

	30 June 2023				30 June 2022			
	Leasehold improvements $'000	Equipment $'000	Appliances $'000	Total $'000	Leasehold improvements $'000	Equipment $'000	Appliances $'000	Total $'000
Cost:								
At 1 July	2,036	13,491	112,301	127,828	-	9,759	92,606	102,365
Additions	1,082	4,038	18,409	23,529	2,036	4,633	24,585	31,254
Disposals	-	(682)	(5,141)	(5,823)	-	(901)	(4,890)	(5,791)
At 30 June	**3,118**	**16,847**	**125,569**	**145,534**	**2,036**	**13,491**	**112,301**	**127,828**
Depreciation:								
At 1 July	-	7,255	60,590	67,845	-	4,987	45,238	50,225
Charge for the period	594	3,773	19,864	24,231	-	2,962	18,355	21,317
Impairment	-	-	52	52	-	-	-	-
Disposals	-	(508)	(3,885)	(4,394)		(694)	(3,003)	(3,697)
At 30 June	**594**	**10,520**	**76,620**	**87,735**	**-**	**7,255**	**60,590**	**67,845**
Net book value as at 30 June	**2,524**	**6,327**	**48,949**	**57,799**	**2,036**	**6,236**	**51,711**	**59,983**

Depreciation of appliances is apportioned to cost of sales based on the proportion of the Company's appliance pool deployed to customer sites in each period, and all appliance depreciation related to customer contracts is recognised in Cost of sales.

Depreciation of appliances used to run Proof of Value ("POV") demonstrations for prospects is apportioned to Sales and marketing based on the proportion of the Company's appliance pool deployed to prospect sites in each period. Where appliances are at client sites or in transit and there is doubt about their recoverability, they are impaired.

The depreciation charges for property plant and equipment have been made in the statement of comprehensive income within the following functional areas:

	FY 2023 $'000	FY 2022 $'000
Depreciation		
Cost of sales	16,667	14,588
Sales and marketing	3,195	3,767
Research and development	913	799
Other administrative	3,456	2,163
Total	**24,231**	**21,317**

13 Leases

Leases

The Company leases various offices and equipment. Rental contracts are typically made for fixed periods of 6 months to 8 years but may have extension options as described below.

Contracts may contain both lease and non-lease components. Under IFRS 16 'Leases' the Company allocates the consideration in the contract to the lease and non-lease components based on their relative stand-alone prices. Lease terms are negotiated on an individual basis and contain a wide range of different terms and conditions. The lease agreements do not impose any covenants other than the security interests in the leased assets that are held by the lessor. Leased assets may not be used as security for borrowing purposes.

Assets and liabilities arising from a lease are initially measured on a present value basis. Lease liabilities include the net present value of the following lease payments:

- fixed payments (including in-substance fixed payments), less any lease incentives receivable,

• variable lease payment that are based on an index or a rate, initially measured using the index or rate as at the commencement date,
• *amounts expected to be payable by the Company under residual value guarantees,*
• the exercise price of a purchase option if the Company is reasonably certain to exercise that option, and
• payments of penalties for terminating the lease, if the lease term reflects the Company's exercising of that option.

Lease payments to be made under reasonably certain extension options are also included in the measurement of the liability. The lease payments are discounted using the interest rate implicit in the lease. If that rate cannot be readily determined, which is generally the case for leases in the Company, the lessee's incremental borrowing rate is used, being the rate that the individual lessee would have to pay to borrow the funds necessary to obtain an asset of similar value to the right-of-use asset in a similar economic environment with similar terms, security and conditions.

To determine the incremental borrowing rate, the Company:
• uses a build-up approach that starts with a risk-free interest rate adjusted for credit risk for leases held by subsidiaries, which do not have recent third-party financing,
• makes adjustments specific to the lease, e.g., term, country, currency, security, and
• if a readily observable amortising loan rate is available to the individual lessee (through recent financing or market data) which has a similar payment profile to the lease, then the Company entities use that rate as the basis to determine the incremental borrowing rate.

Right-of-use assets
Right-of-use assets are measured at cost considering the following:
• the amount of the initial measurement of lease liability,
• any lease payments made at or before the commencement date less any lease incentives received,
• any initial direct costs, and
• restoration costs.

Right-of-use assets are generally depreciated over the shorter of the asset's useful life (typically first expected break clause to be executed if this is expected) and the lease term on a straight-line basis. If the Company is reasonably certain to exercise a purchase option, the right-of-use asset is depreciated over the underlying asset's useful life.

Payments associated with short-term leases of equipment and all leases of low-value assets are recognised on a straight-line basis as an expense in the statement of comprehensive income. Short-term leases are leases with a lease term of 12 months or less without a purchase option. Low-value assets are generally comprised of IT equipment and small items of office furniture.

Extension and termination options
Extension and termination options are included in several property and equipment leases across the Company. These are used to maximise operational flexibility in terms of managing the assets used in the Company's operations. Most of the extension and termination options held are exercisable only by the Company and not by the respective lessor.

Right-of-use asset capitalised on the statement of financial position are as below:

	30 June 2023 $'000	**30 June 2022 $'000**
Cost		
1 July	27,680	19,176
Additions	53	9,538
Impairment	(1,781)	-
Disposal	(1,407)	(1,034)
30 June	24,545	27,680
Depreciation		
As at 1 July	9,415	7,170
Charge for the period	3,813	2,704
Disposal	(1,407)	(459)
30 June	11,821	9,415
Net book value at 30 June	**12,724**	**18,265**

The depreciation charges for right-of-use assets have been made in the statement of comprehensive income within the following functional areas:

	FY 2023 $'000	FY 2022 $'000
Depreciation		
Sales and marketing	2,468	1,763
Research and development	578	395
Other administrative	767	546
Total	**3,813**	**2,704**

Lease liabilities are presented in the statement of financial position as follows:

	30 June 2023 $'000	30 June 2022 $'000
Current	873	1,153
Non-Current	19,402	19,402
Total	**20,275**	**20,555**

The Company has leases for office space around the world. With the exception of short-term leases and leases of low value underlying assets, each lease is reflected on the statement of financial position as a right-of-use asset and a lease liability.

The Company must keep the offices it leases in a good state of repair and return the offices in a condition as good as their original condition at the end of the lease. Further, the Company must ensure any leasehold improvements made to the offices and incur servicing fees in accordance with the lease contracts.

The following table describes the nature of the Company's leasing activities by type of right-of-use asset recognised on the statement of financial position:

Year	Right-of-use asset	No. of right-of-use assets leased	Range of remaining term	Average remaining lease term	No. of leases with extension options	No. of leases with early break clause
30 June 2022	Office space	9	1-11 years	8 years	2	3
30 June 2023	Office space	7	1-11 years	5 years	2	6

The lease liabilities are secured by the related underlying assets. The table below shows undiscounted lease maturity analysis:

Lease maturity analysis	30 June 2023 $'000	30 June 2022 $'000
Lease liabilities, short term	1,812	2,617
1 – 2 years	5,429	5,200
2 – 5 years	15,298	15,044
Over 5 years	-	1,435
Total	**22,539**	**24,296**

The Company has elected not to recognise a lease liability for short term leases (leases with an expected term of 12 months or less) or for leases of low value assets. Payments made under such leases are expensed as incurred. The expense relating to payments not included in the measurement of the lease liability is disclosed below:

	FY 2023 $'000	FY 2022 $'000
Short term leases	1,294	1,498
Low value lease rentals	32	1,050
Total	**1,326**	**2,548**

The Company also holds leases for office equipment such as photocopiers for which it has taken the small value exemption.

14 Capitalised commission

Commission cost recognition
Commission costs are all recognised as Sales and marketing costs. IFRS 15 requires that certain costs incurred in both obtaining and fulfilling customer contracts be deferred on the statement of financial position where recoverable and amortised over the period that an entity expects to benefit from the customer relationship. The only significant cost falling within the remit of IFRS 15 is the portion of commission costs classified as a cost of contract acquisition. Depending on their role in sales, staff receive either the first 50% or 100% of commission at the point of contract signing, which is deemed to meet the criteria of being incurred solely to acquire the contract. These transaction related commission costs, including related social security and similar contributions, are therefore capitalised and amortised over the customer contract term, with the amortisation being recognised as a Sales and marketing cost. Commissions paid to referral partners are also capitalised and amortised to Sales and marketing costs over the life of the related contracts.

The remaining 50% of sales staff commission is paid on the earlier of the full contract value being paid, or, most frequently, after one year. Because these commissions have additional service and performance requirements, they are not eligible to be capitalised under IFRS 15. Instead, the commission and associated social security costs are accrued based on the expected period between the sale and payment, then the accrual is released when the commission is paid or earlier if commission is recouped due to the customer defaulting on payments or salesperson ceases to be employed prior to the commission becoming payable.

Refer to note 2 for impairment of non-financial asset.

Capitalised commissions, which primarily represent approximately 50% of commissions paid to the Company and subsidiaries' salesforce and partners, are deemed to be a cost of obtaining a contract and are spread over the expected contact term.

By geographic market	30 June 2023 $'000	30 June 2022 $'000
USA	23,303	17,321
United Kingdom	10,933	10,142
Europe	23,742	17,060
Rest of World	18,675	12,631
	76,653	**57,154**
Current	34,471	24,635
Non-current	42,182	32,519
	76,653	**57,154**

	FY 2023 $'000	FY 2022 $'000
Amortisation in the year	32,471	21,817
Impairment in the year	1,555	996

15 Investments

Investments accounting policy
Investments in subsidiaries are recorded at cost, which is the fair value of the consideration paid.

The cost related to the subsidiaries' employees service in connection to share based payments granted before IPO and for periods before IPO, is treated as investment value in subsidiaries. The awards represent capital contribution to the subsidiaries as no payment is expected for the equity-settled share-based payment awarded to their employees.

Investments are tested for impairment whenever events or changes in circumstances indicate that the carrying amount may not be recoverable. An impairment loss is recognised for the amount by which the asset's carrying amount exceeds its recoverable amount. The recoverable amount is the higher of an asset's fair value less costs of disposal and value in use. For the purposes of assessing impairment, assets are grouped at the lowest levels for which there are separately identifiable cash inflows which are largely independent of the cash inflows from other assets or groups of assets (cash-generating units). Investments that suffered an impairment are reviewed for possible reversal of the impairment at the end of each reporting period.

	30 June 2023 $'000	30 June 2022 $'000
Opening value	**64,252**	**10,807**
Acquisition of Cybersprint B.V.	-	51,958
Capital contribution related to share-based payment	-	1,487
Investments in subsidiaries incorporated during the year	79	-
Carrying value	**64,331**	**64,252**

Investment in subsidiaries incorporated in FY 2023

The capital contribution relates to the incorporation of Darktrace Korea Limited and Darktrace Sweden AB during the year.

Acquisition in FY 2022

On 1 March 2022 Darktrace acquired the entire issued share capital of Cybersprint B.V. ("Cybersprint"), an attack surface management company that provides continuous, real-time insights from an outside-in perspective to eliminate blind spots and detect risks. The acquisition of Cybersprint is aligned with Darktrace's vision of delivering a 'Continuous Cyber AI Loop' and complements its Self-Learning technology and inside-out view. On 16 January 2023 Cybersprint B.V. changed its name to Darktrace Netherlands B.V.

Darktrace acquired Cybersprint for €47.5 million ($53.7 million), paid 75% in cash and 25% in equity. Following adjustments for cash balances, third party debt and working capital the consideration has been adjusted to $36.1 million cash consideration and $8.2 million equity consideration. In particular certain shares issued were treated as a remuneration under IFRS 2- Share-based payment (note 21).

Equity instruments issued

2,573,648 shares in Darktrace plc were issued as consideration to the Sellers (Cybersprint shareholders before acquisition). The fair value of the acquirer's equity interests issued is determined as consideration for the acquired business. Fair value is the quoted share price, on the acquisition date (£4.59/ $6.15), multiplied by the number of shares issued for publicly traded shares. These are treated as a capital contribution to Darktrace Holdings Limited as they were treated as consideration towards the acquisition of Cybersprint.

Acquisition related costs

The Company incurred acquisition related cost of $0.9 million related to legal and professional fees. These costs were included in administrative expenses in the statement of comprehensive income.

As at 30 June 2023, the subsidiaries owned by the Company were as follows:

Subsidiary	Country of registration	Registered office	Year of incorporation	Class of share capital held	Proportion held
Darktrace, Inc	USA	C/O Paracoprt Incorporated, 2140 S DuPont Highway, Camden, Delaware 19934, USA	2013	Common shares	100%
Darktrace Singapore Pte Ltd.	Singapore	4 Shenton Way, #28-03 SGX Centre 2, Singapore 068807	2015	Common shares	100%
Darktrace Australia Pty Ltd.	Australia	C/O BP Woodward & Associates, Level 5 Suite 501, 83 York Street, Sydney NSW 2000, Australia	2015	Common shares	100%
Darktrace Japan KK	Japan	12-1-605 Okahigashi-cho, Hirakata City, Osaka, Japan	2017	Common shares	100%
Darktrace South Africa Pty Ltd	South Africa	BDO Building, Wanderers Office Park, 52 Corlett Drive, Illovo, Gauteng, 2196	2016	Common shares	100%
Darktrace Ireland Limited	Ireland	38 Upper Mount Street, Dublin 2, Dublin, Ireland	2019	Common shares	100%
Darktrace SaS	France	38 avenue des Champs-Élysées. 75008 Paris	2019	Common shares	100%
Darktrace Hong Kong Ltd	Hong Kong	31/F Tower Two Time Square, Matheson Street, Causeway Bay, Hong Kong	2019	Common shares	100%
Subsidiary	**Country of registration**	**Registered office**	**Year of incorporation**	**Class of share capital held**	**Proportion held**

Darktrace Colombia SaS	Colombia	Cra 16 # 97 – 46 Torre 1 piso 6, Bogota, Colombia	2019	Common shares	100%
Darktrace Canada, Inc	Canada	585 16th Street, Suite 201, West Vancouver, British Columbia, V7V 3R8, Canada	2020	Common shares	100%
Darktrace Mexico, SA De CV	Mexico	Boulevard Manuel Ávila Camacho No 76 PB Colonia: Lomas de Chapultepec Alcaldía: Miguel Hidalgo Ciudad de Mexico C.P.11000	2020	Common shares	100%
Darktrace GmbH	Germany	Nonnenbrücke 12, 96047 Bamberg, Germany	2020	Common shares	100%
Darktrace Netherland B.V.	Netherlands	Wilhelmina van Pruisenweg 35, (2595 AN) The Hague, the Netherlands	2022	Common shares	100%
Darktrace Korea Limited	South Korea	4th Floor, LS YongSan Tower, 92, Hangang-daero, Yongsan-gu, Seoul, Republic of Korea, 04386	2022	Common shares	100%
Darktrace Sweden AB	Sweden	C/O TMF Sweden AB, Sergels Torg 12, 111 57 Stockholm	2022	Common shares	100%

16 Trade and other receivables

Trade receivables are recognised initially at the amount of consideration that is unconditional, unless they contain significant financing components when they are recognised at fair value. They are subsequently measured at amortised cost using the effective interest method, less expected credit loss provision.

The Company has adopted the simplified model of recognising lifetime expected credit losses for all trade receivables on a collective basis as there are shared credit risk characteristics, grouped on basis of geography and days past due. The amount of the provision is determined as the difference between the asset's carrying amount and the present value of estimated future cash flows, discounted using the original effective interest rate. See note 16 for a description of the Company's impairment policies.

The Company writes off trade receivables when in its view there is no reasonable expectation of recovery.

Short term deposits represent the short-term portion of deposits mostly related to lease deposits for the Company's offices or future marketing events.

Deposits
Deposits are financial assets at amortised cost, primarily related to cash deposits in connection to leases for the Company's offices. Where the agreement is for a term longer than one year, the related deposit is classified as long term. Refer to note 17 for accounting treatment of short-term deposits instead.

	30 June 2023 $'000	30 June 2022 $'000
Trade receivables	92,912	63,795
Prepayments	17,845	16,984
Accrued income	3,445	4,152
Deposits	834	528
Other receivables	1,518	368
Amounts owed by entities under common control	217	-
Amounts owed by subsidiary undertakings	9,459	18,495
Total	**126,230**	**104,322**

The carrying value of trade receivables is considered a reasonable approximation of fair value due to the short-term nature of the balance.

The Company applies the IFRS 9 simplified approach to measuring expected credit losses which uses a lifetime expected loss allowance for all trade receivables. To measure the expected credit losses, trade receivables have been grouped based on shared credit risk characteristics and the days past due. The expected loss rates are based on the payment profiles of receivables in a 36-month period before 30 June 2023 and 30 June 2022, and the corresponding historical credit losses experienced within these periods. Historic loss rates are adjusted to reflect current and forward-looking information on macro-economic and other factors affecting the ability of customers to settle the receivables.

The Company has recorded an expected credit loss provision for trade receivables as determined under the requirements of IFRS 9, at 30 June 2023 of $ 5.2 million (30 June 2022 of $3.1 million).

The movement in the credit loss provision is as follows:

	FY 2023 $'000	FY 2022 $'000
At the beginning of the period	3,119	5,461
Charge for the period	3,954	1,872
Reversal on collected amounts	(1,905)	(2,795)
Amounts written off	-	(1,419)
Expected credit loss provision at end of the period	**5,168**	**3,119**
Receivables written off during the period	1,024	2,608

The net movement in the expected credit loss provision has been included in administrative expenses in the statement of comprehensive income.

The expected credit loss for trade receivables was determined as follows:

30 June 2023	**Up to 30 days $'000**	**Up to 60 days $'000**	**Up to 90 days $'000**	**More than 90 days $'000**	**Total $'000**
Expected credit loss rate	0.9%	3.2%	20.6%	73.3%	5.0%
Gross carrying amount for trade receivables and accrued income	88,092	6,810	2,471	4,985	102,358
Lifetime expected credit loss	**(789)**	**(219)**	**(508)**	**(3,652)**	**(5,168)**
30 June 2022					
Expected credit loss rate	0.2%	2.6%	23.2%	76.3%	4.4%
Gross carrying amount for trade receivables and accrued income	63,464	3,608	1,230	3,399	71,701
Lifetime expected credit loss	**(149)**	**(92)**	**(285)**	**(2,593)**	**(3,119)**

17 Cash and cash equivalents

Cash and cash equivalents
Cash and cash equivalents includes cash on hand, other short-term, highly liquid investments with original maturities of three months or less that are readily convertible to known amounts of cash and which are subject to an insignificant risk of changes in value.

Deposits at call are presented as cash equivalents if they have a maturity of three months or less from the date of acquisition and are repayable with 24 hours' notice with no loss of interest.

	30 June 2023 $'000	30 June 2022 $'000
Cash at bank and in hand	83,485	91,914
Deposits at call	124,195	65,094
Cash and cash equivalents	**207,680**	**157,008**

18 Trade and other payables

These amounts represent liabilities for goods and services provided to the Company prior to the end of the financial year or any other period which are unpaid. The amounts are unsecured and are usually paid within 30 days of recognition. Trade and other payables are presented as current liabilities unless payment is not due within 12 months after the end of the reporting period. They are recognised initially at their fair value and subsequently measured at amortised cost using the effective interest method.

Commission accruals
For certain sales staff, the second 50% of sales commission is paid at the earlier of full payment of the contract or most frequently, after one year. As payment requires additional service and performance requirements, this cost is not eligible to be capitalised. This cost is accrued over the expected period between the sale and the payment to the sales staff, with the accrual released when the commission is paid or earlier if commission is recouped due to customer defaulting on payments. Estimation of the effect of leavers has been incorporated into the commission accrual calculation in-line with IAS 19 'Employee Benefits'.

Amounts falling due within one year:

	30 June 2023 $'000	30 June 2022 $'000
Trade payables	12,604	10,400
Social security and other taxes	10,168	15,394
Accruals	74,024	50,695
Amounts owed to subsidiary undertakings	826	29,271
As at 30 June	**97,622**	**105,760**

Accruals includes mainly:

- $52.9 million accrued commission and sales bonus (30 June 2022: $33.9 million): $25.7 million (30 June 2022: $14.8 million) relates to Company employees and $27.2 million (30 June 2022: $19.1 million) is an intercompany balance as it relates to subsidiaries' employees.
- $8.8 million accrued salaries and partner fees (30 June 2022: $5.9 million)
- $7.0 million accrued hosting fees and professional fees including audit and accountancy (30 June 2022: $5.0 million)
- $2.3 million accrued marketing and recruitment costs (30 June 2022: $3.9 million)
- $1.2 million accrued NI social security on salaries (30 June 2022: $0.7 million)
- $1.0 million accrued legal fees (30 June 2022: $1.3 million)

19 Provisions

Dilapidation provision
Darktrace is required to restore the leased premises of its offices to their original condition at the end of the respective lease terms. A provision has been recognised for the present value of the estimated expenditure required to remove any leasehold improvements. These costs have been capitalised as part of the right-of-use asset and are amortised over the term of the lease.

The Company accounts for a provision on tax payments when the employer has primary liability to pay for social security-type contribution on share-based payments. In some jurisdictions, the employer rather than the employee has the legal obligation to pay taxes on employee awards. Darktrace Holdings Limited recognises the cost and liability in relation to those countries where this type of payments is required. Management calculates the liability arising from the obligation to pay taxes as a provision in accordance with IAS 37 using the market value of the total options at each reporting date to estimate the provision to be accrued over the vesting period. Also, provisions are recognised where a legal or constructive obligation exists at the balance sheet date, as a result of a past event, where the amount of the obligation can be reliably estimated and where the outflow of economic benefit is probable.

Significant estimate in the share price used to calculate the provision for share-option related employer tax charges
The provision represents the best estimate of the amount payable by the Company at year end if all options were exercised at that date. The key input for the calculations is the percentage applicable for each country and the share price at each period end. The key element subject to change in future periods is the share price, and for this reason the Company has prepared the following sensitivity analysis:

	30 June 2023 $'000	30 June 2022 $'000
+/- 10% share price value – change in value of accrual ($'000 absolute value)	612	3,112

			30 June 2023			30 June 2022
	Share-based payment tax $'000	Other provision $'000	Total provision $'000	Share-based payment tax $'000	Other provision $'000	Total provision $'000
Opening provision	12,236	2,100	14,336	17,628	0	17,628
Reclassification from accruals						
Accrual for the year	4,139	(854)	3,285	519	2,100	2,619
Utilisation	(12,737)	-	(12,737)	(5,911)	-	(5,911)
Closing provision	**3,638**	**1,246**	**4,884**	**12,236**	**2,100**	**14,336**
Current	3,610	1,246	4,856	11,842	-	11,842
Non-current	28	-	28	394	2,100	2,494
Total provision for share-option related employer tax charges	**3,638**	**1,246**	**4,884**	**12,236**	**2,100**	**14,336**

The Company accounts for a provision on tax payments when employer has primary liability to pay for social security-type contribution on share-based payments at the time of exercise.

In the UK, an award of shares or options to an employee gives rise to a personal tax liability for the employee, related to the fair value of the award when it vests.

Other provision includes an estimate of tax charges related to new permanent establishments in countries where Darktrace plc does not currently have a subsidiary and provision for dilapidation previously classified within lease liabilities.

20 Share capital and share premium

Contributed equity

Ordinary shares are classified as equity. Incremental costs directly attributable to the issue of new shares or options are shown in equity as a deduction, net of tax, from the proceeds.

Equity comprises the following:

- Share capital: represents the nominal value of equity shares.
- Share premium: represents the excess over nominal value of the consideration received for equity shares, net of any transaction costs associated with the issue of shares.
- Stock compensation reserve: this reserve is used to recognise the grant date fair value of options issued to employees but not exercised, the grant date fair value of growth shares issued to employees and the grant date fair value of deferred shares granted to employees but not yet vested. This reserve was used to recognise the grant date fair value of options and awards issued to the Company' employees up to the date of share for share exchange, date at which all outstanding options were transferred to Darktrace plc.
- Capital contribution: When Darktrace plc (parent company) grants rights to its equity instruments to employees of its subsidiary (Darktrace Holdings Limited), the subsidiary does not have an obligation to provide its parent's equity instruments to its employees. The subsidiary should, in its own separate financial statements, measure the services received from its employees in accordance with the requirements of IFRS 2 applicable to equity-settled share-based payment transactions. There will be a corresponding increase recognised in equity as a capital contribution from the parent company. Since the transfer of all options to Darktrace plc, a capital contribution corresponding to the cost of the service provided by an employee is accounted for by the Company for any new awards provided.
- Foreign currency translation reserve: relates to historical balance which resulted from consolidation as a result of translating the financial statement items from the functional currency into the presentational currency using the exchange rate at the statement of financial position date in the prior years.
- Retained earnings: represents retained profits and losses.

Share capital	No. of ordinary shares of £0.01 each	No. of preference shares of £1 each	No. of deferred shares of £0.01 each	Growth shares	Total no. of shares	Share capital $'000	Share premium $'000
1 July 2021	567,781,092	-	120,063	-	567,901,155	31	313,611
Issuance of preference shares	-	50,000	-		50,000	69	-
Subdivision & conversion of preference shares into ordinary	1,250,000,000	(50,000)	-	-	1,249,950,000	-	-
Subdivision & conversion of deferred shares into ordinary	30,015,750	-	(120,063)	-	29,895,687	-	-
30 June 2022	**1,847,796,842**	-	-	-	**1,847,796,842**	**100**	**313,611**
1 July 2022	1,847,796,842	-	-	-	1,847,796,842	100	313,611
30 June 2023	**1,847,796,842**	-	-		**1,847,796,842**	**100**	**313,611**

Transactions in prior year

Share sub-division and share conversion

On 18 October 2021, the redeemable preference and deferred shares in Darktrace Holdings Limited were subdivided by 250 and converted into ordinary shares in Darktrace Holdings Limited.

Transactions in the year

In the UK, an award of shares or options to an employee gives rise to a personal tax liability for the employee, related to the fair value of the award when it vests. In order to meet this tax liability, two executives surrendered as many shares as are needed to raise proceeds equal to the tax liability ('net settlement'). This tax collection arrangement meant that the equity–settled awards resulted in a debit to the equity of the Company for the income tax for $9.7 million and a liability to pay for the tax which has been paid in the year.

21 Share-based payments

Share-based payments

The parent company operates an equity settled share-based payment scheme. The equity settled share-based payments are measured at fair value at the date of grant. Having a graded vesting schedule, the fair value determined is expensed on a straight-line basis over the requisite service period for each separately vesting portion of the award as if the award was, in-substance, multiple awards. The charge for the period is allocated to the relevant income statement categories where the employment costs of the employee who is granted the equity options are charged.

The fair value of options and awards granted is recognised as an employee benefits expense, with a corresponding increase in equity. The total amount to be expensed is determined by reference to the fair value of the options granted,

- including any market performance conditions (e.g. the parent company's share price)
- excluding the impact of any service and non-market performance vesting conditions (e.g. profitability, sales growth targets and remaining an employee of the entity over a specified time period), and
- including the impact of any non-vesting conditions (e.g. the requirement for employees to save or hold shares for a specific period of time).

The total expense is recognised over the vesting period, which is the period over which all of the specified vesting conditions are to be satisfied. At the end of each period, the Company revises its estimates of the number of options that are expected to vest based on the non-market vesting and service conditions. It recognises the impact of the revision to original estimates, if any, in profit or loss, with a corresponding adjustment to equity. When the options are exercised, the appropriate number of shares is issued to the employee. The proceeds received, net of any directly attributable transaction costs, are credited directly to equity.

Modification of share-based payments

Where the effect of the modification is to increase the value of the award to an employee, the incremental fair value is recognised as a cost. The incremental fair value is the difference between the fair value of the original award and that of the modified award, both measured at the date of modification.

Share-based payment charges have been made in the statement of comprehensive income within the following functional areas.

	FY 2023 $'000	FY 2022 $'000
Sales and marketing	8,090	17,105
Research and development	4,883	8,789
Other administrative	9,367	5,706
Total share-based payment expense	**22,340**	**31,600**

Share-based payments are calculated in accordance with IFRS 2 – Share-based Payment. The Company has used a Black-Scholes valuation model to value the options and growth shares granted up to the IPO and a Monte Carlo Model for the AIP awards granted at IPO. Where an option scheme has no market-based performance conditions attached to the award, a Black-Scholes model is typically appropriate. The growth shares have a hurdle, which is a market-based performance condition, however, this is used a proxy for exercise price. Therefore, Black-Scholes is still an appropriate model.

Option schemes in place before IPO

Share options are exercisable at prices determined at the date of grant. All awards vest over three years from the grant date in six-month intervals, (i.e. 1/6 of the Awards will vest every six months over 36 months) subject to continued employment.

Movements in the number of share options outstanding is as follows:

	FY 2023 Options Number	FY 2022 Options Number
Outstanding at 1 July	23,280,395	31,567,011
Lapsed	(87,529)	(236,842)
Exercised	(6,185,982)	(8,049,774)
Outstanding at 30 June	**17,006,884**	**23,280,395**
Exercisable at 30 June	**15,401,497**	**18,772,832**

The table below presents the weighted average remaining contractual life ('WACL') and the price range for the options outstanding at each period end:

		30 June 2023		30 June 2022
Range of exercise prices	**WACL**	**Options number**	**WACL**	**Options number**
$0.00 to $0.23	1.45	3,385,583	7.00	6,122,124
$0.36 to $0.67	3.18	2,345,092	4.18	3,599,261
$1.21 to $1.45	4.45	944,737	5.45	1,468,044
$1.85 to $2.21	4.89	1,113,934	5.89	1,229,379
$2.47 to $2.87	5.79	4,955,535	6.77	6,457,419
$5.20	7.33	4,262,003	8.72	4,404,168
	6.01	**17,006,884**	**7.01**	**23,280,395**

AIP awards

Performance based conditional award (the 'Performance Awards')

Vesting of Tranche 1 is dependent on Darktrace's total shareholder return ('TSR') performance over the period from the Admission Date to the end of the Financial Year 2023, ranked in comparison to the constituents of the FTSE 350 (ex. Investment companies). Tranche 2 vests dependent on the same terms, albeit the measurement period runs from the Admission Date to the end of the Financial Year 2024 (i.e. an additional year). Awards do not incorporate an exercise price.

Awards issued during the year also have market-based vesting criteria with up to 80% of the awards vesting in accordance with the conditions of the TSR Tranche. Tranche 2 vests depending on ARR growth targets at the end of the performance period.

Executive director conditional awards ('Executive Awards')

The Executive Awards carry the same market-based vesting criteria as Tranche 2 of the Performance Awards. Additionally, they have a holding period which determines vested shares must be retained for a period of five years from grant. Awards do not incorporate an exercise price.

Top-up awards and modification

These awards vest according to a share price performance hurdle measured over a one-year period following the Admission Date. In essence, no shares vest where the closing share price is £2.50 or less, where closing share price is £5, 100% of the shares vest and where the closing share price is between £2.50 and £5 the number of awards vests on a straight-line basis. Awards do not incorporate an exercise price.

The performance period for the vesting of Top-Up awards ended on 6 May 2022 with the original calculation based on the share price for the 30-days up to the 6 May 2022. Management determined that a much longer measurement period was needed to ensure that the share price used to determine vesting of the awards reflects Management 's performance and the underlying performance of the business. Management offered a modification to the employees to extend the performance averaging period to 12 months ending on the first anniversary of IPO resulting in 100% of the award vesting but extending the service period to 31 October 2022.

The effect of the modification is to increase the value of the award to the employees through removal of market condition and allowing the employee to have the maximum number of shares although with a small extension of the employment period i.e. vesting period, the incremental fair value increase must be recognised as a cost over the vesting period. The incremental fair value is the difference between the fair value of the original award (measured using the Monte Carlo model) and that of the modified award (time-based award means the valuation is the share price at grant date), both measured at the date of modification. There were no compensation payments for this modification.

Time-based awards

These awards vest according to time only. There is no market-based vesting criteria and awards do not incorporate an exercise price. The value of the time-based awards will simply be the value of the underlying equity.

Modification to the top-up awards

The performance period for the vesting of Top-Up awards ended on 6 May 2022 with the original calculation based on the share price for the 30-days up to the 6 May 2022. Management determined that a much longer measurement period was needed to ensure that the share price used to determine vesting of the awards reflects management's performance and the underlying performance of the business. Management offered a modification to the employees to extend the performance averaging period to 12 months ending on the first anniversary of IPO resulting in 100% of the award vesting but extending the service period to 31 October 2022.

The share option schemes and awards are accounted for as equity settled share-based payment transactions.

Movements in the number of share awards outstanding are as follows:

	FY 2023	FY 2022
Outstanding at 1 July	17,525,519	16,399,584
Granted	5,250,395	1,437,303
Lapsed	(463,850)	(197,646)
Exercised	(15,119,262)	(113,722)
Outstanding at 30 June	**7,192,802**	**17,525,519**
Exercisable at 30 June	**7,492**	-

22 Capital commitments

The Company had no capital commitments at 30 June 2023 or 30 June 2022.

23 Deferred tax assets and liabilities

For details on significant judgement and estimate in deferred tax asset (DTA) recognised on UK losses carried forward refer to note 10.

The unrecognised deferred tax asset is comprised of:

		30 June 2023		30 June 2022
	Gross amounts	Unrecognised DTA	Gross amounts	Unrecognised DTA
	$'000	$'000	$'000	$'000
Fixed Asset timing differences	-	-	(2,152)	(538)

Short term temporary differences	3,401	850	17,224	4,306
Losses	200,880	50,220	206,660	51,665
Share based payments	48,747	12,187	99,708	24,927
Total	**253,028**	**63,257**	**321,440**	**80,360**

Given the uncertainty of the tax deduction in excess of the IFRS2 charge recognised for share-based payments, demonstrated by the high volatility of Darktrace plc share price since IPO, the related deferred tax asset has not been recognised at 30 June 2023 or in the prior year.

Recognised deferred tax asset and liabilities:

	30 June 2023 $'000	30 June 2022 $'000
Fixes Asset Timing Differences	(2,183)	(961)
Short Term temporary differences	2,183	961
Losses	10,900	-
Total	**10,900**	-

Movement in deferred tax asset:

	FY 2023 $'000	FY 2022 $'000
Opening	-	-
(charged)/credited to income statement:		
deferred tax asset movement	10,900	-
Closing	**10,900**	-

24 Related parties

As a wholly owned subsidiary of Darktrace plc, the Company has taken advantage of the exemption contained in FRS 101 and has therefore not disclosed transactions or balances with wholly owned subsidiaries of Darktrace plc.

Other related party disclosures
Other related parties include transactions with companies under common directorship and revenues from investors and affiliated companies.

	Transaction value		Balances outstanding	
	FY 2023 $'000	FY 2022 $'000	FY 2023 $'000	FY 2022 $'000
Fees for management support services	-	-	43	-
Recharge of staff expenditure	-	1	-	-
Income from recharge of office space	-	(270)	-	-
Revenue received	(734)	(712)	(235)	(249)
Hosting Fees	-	7	1	1
	(734)	**(974)**	**(191)**	**(248)**

25 Ultimate controlling party

The ultimate parent undertaking and the smallest and largest Company to consolidate these financial statements is Darktrace plc. Copies of Darktrace plc's Annual Report are publicly available: https://ir.darktrace.com/financial-results.

26 Post balance sheet events

Assignment of previous London office lease

On 4 August 2023 the assignment of the lease for the previous London office has been completed. This will result in the derecognition of the related right-of-use asset of $2.7 million and the de-recognition of the lease liability of $3.9 million as at the date of assignment.

RCF extension

On 31 August 2023 the RCF agreement with Silicon Valley Bank (now HSBC Innovation Bank) has been extended to have an expiry date of 30 November 2023. All other terms and conditions (see note 20) remain unchanged. The company is currently considering the proposals from a number of financial institutions to increase the amount of the facility before the end of the agreement with HSBC Innovation Bank.