RG
Ryecroft Glenton

mercia
asset management

North East

M&A Technology Sector Snapshot

Oct-22 to Dec-22

Contents

RG
Ryecroft Glenton

mercia
asset management

Key M&A Headlines

Most active M&A sectors by volume of deals done

(Oct-22 to Dec-22)

Business/Productivity Software - 184

Financial Software - 101

IT Consulting and Outsourcing -53

Media and Information Services (B2B) - 41

Entertainment Software - 24

Educational Software - 21

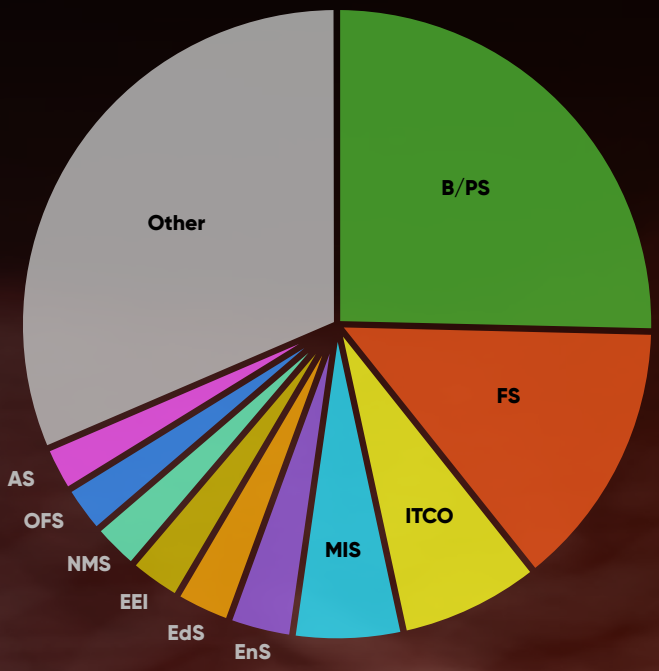
Electronic Equipment and Instruments - 20

Network Management Software - 18

Other Financial Services - 18

Application Software -17

Other - 228



Most active M&A regions by volume of deals done

(Oct-22 to Dec-22)

London - 366

Manchester - 21

Cambridge - 17

Bristol - 13

Edinburgh - 12

Oxford - 8

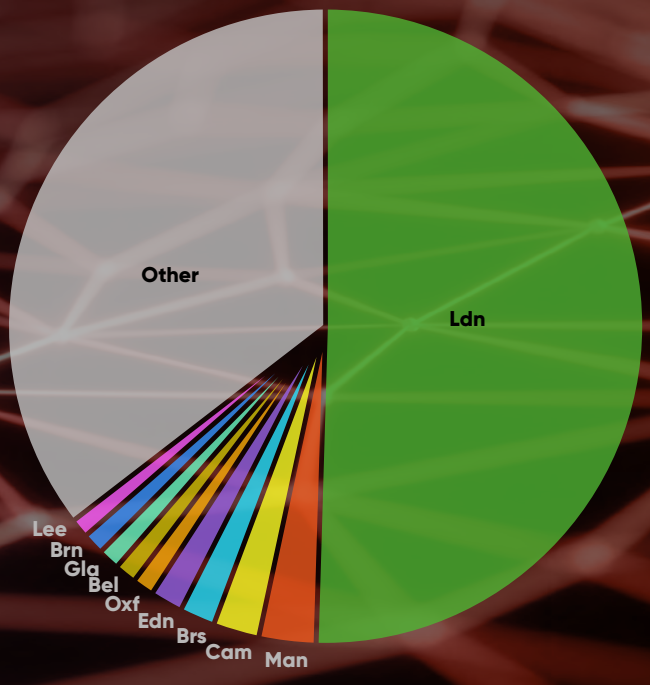
Belfast - 8

Glasgow - 8

Brighton - 8

Leeds - 7

Other - 257



Total deals in the 'technology' sector in UK (Oct-22 to Dec-22)

725 Deals

Source – MarketIQ

Introduction

Welcome to the eighth edition of the North East: M&A Technology Sector Snapshot – a joint production from Ryecroft Glenton and Mercia Asset Management PLC.

We publish a snapshot each quarter to provide information on national themes in the UK tech sector, as well as focusing on developments closer to home, in the North East.

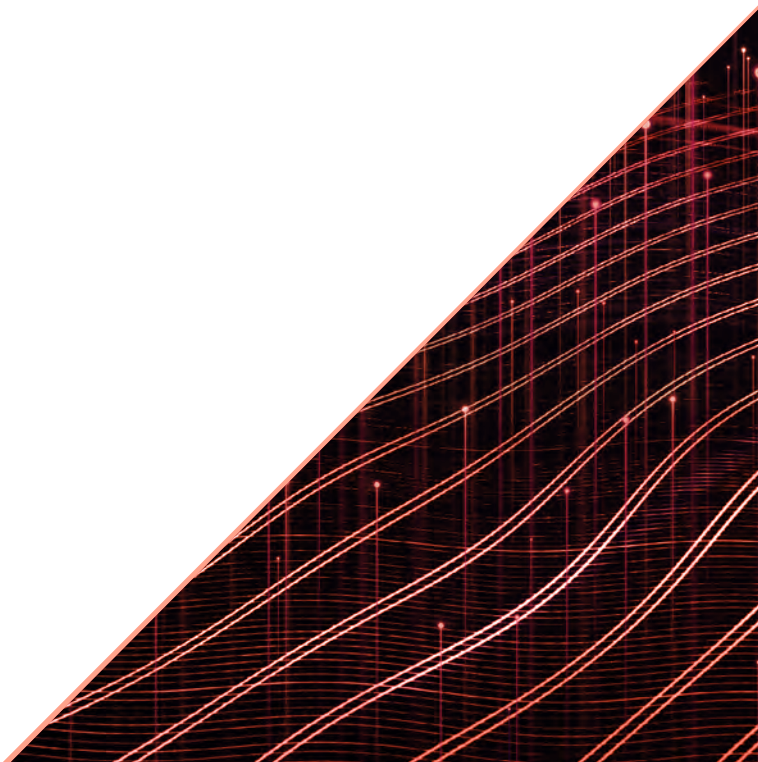
The snapshot provides an insight into key industry trends, current market data, news, and an overview of recent transactions. In this issue, the deal round-up covers the three months from October 22 to December 22.

Each quarter we shine the spotlight on a specific sub-sector within the technology industry. This quarter we take a closer look at the Cybersecurity sector.

The UK tech market continues to be very active with 725 deals recorded between October 2022 to December 2022, with approximately 30% relating to an acquisition or a sale, and circa 68% relating to a funding round. Business/Productivity Software is the most active tech sub-sector for M&A in Q4 22 and London continues to lead the way geographically, with 366 deals completed in the quarter.

Quarter	Total Deals (UK)	Total deals (North East)	Most active region of total deals	North East share of deals	Most active sector
Q4 - 22	725	6	London (366 deals)	c.1%	Business/Productivity Software (8.59%)
Q4	4,595	78	London (2,769 deals)	c.1.6%	Business/Productivity Software (18.6%)

Sources – Pitchbook



The UK tech market continues to be very active with 725 deals recorded between October 2022 to December 2022.

RG
RyecroftGlenton

mercia
asset management

A General Technology Sector News Round Up

National

UK 'top-attacked' country in Europe for cyberattacks in 2022

- The UK was the 'top-attacked' country in Europe by cyberattacks in 2022, according to a new report.
- A study from IBM has indicated that the UK accounted for 43 per cent of cyberattacks in 2022. Germany was placed second at 14 per cent, and Portugal was third at nine per cent.

Article available here: https://nationaltechnology.co.uk/UK_topattacked_country_in_Europe_for_cyberattacks_in_2022.php

Europe's Digital Markets Act (DMA) Takes a Hammer to Big Tech

- The EU targets tech giants' walled gardens with aggressive new rules, but the smaller companies the DMA is meant to help are sceptical it will work.

Article available here: https://www.wired.co.uk/article/digital-markets-act-messaging

Challenger banks surpass high street lenders for SME loans

- Challenger and specialist banks have surpassed high street banks for smaller business lending, with new data showing they accounted for 55% of the SME market in 2022.

Article available here: https://www.uktech.news/fintech/challenger-bank-lending-20230301

North East

Regional spotlight: The rise of North East tech – and its growth potential

- Data collected by credit report agency CreditSafe found that entrepreneurs launched more than 12,000 startups across the region last year. The region's key tech hotspots include Newcastle, Middlesbrough, Durham, Sunderland and Northumberland.

Article available here: https://www.uktech.news/partnership/regional-spotlight-north-east-20230301

CEO unveils bright future for tech champions Dynamo

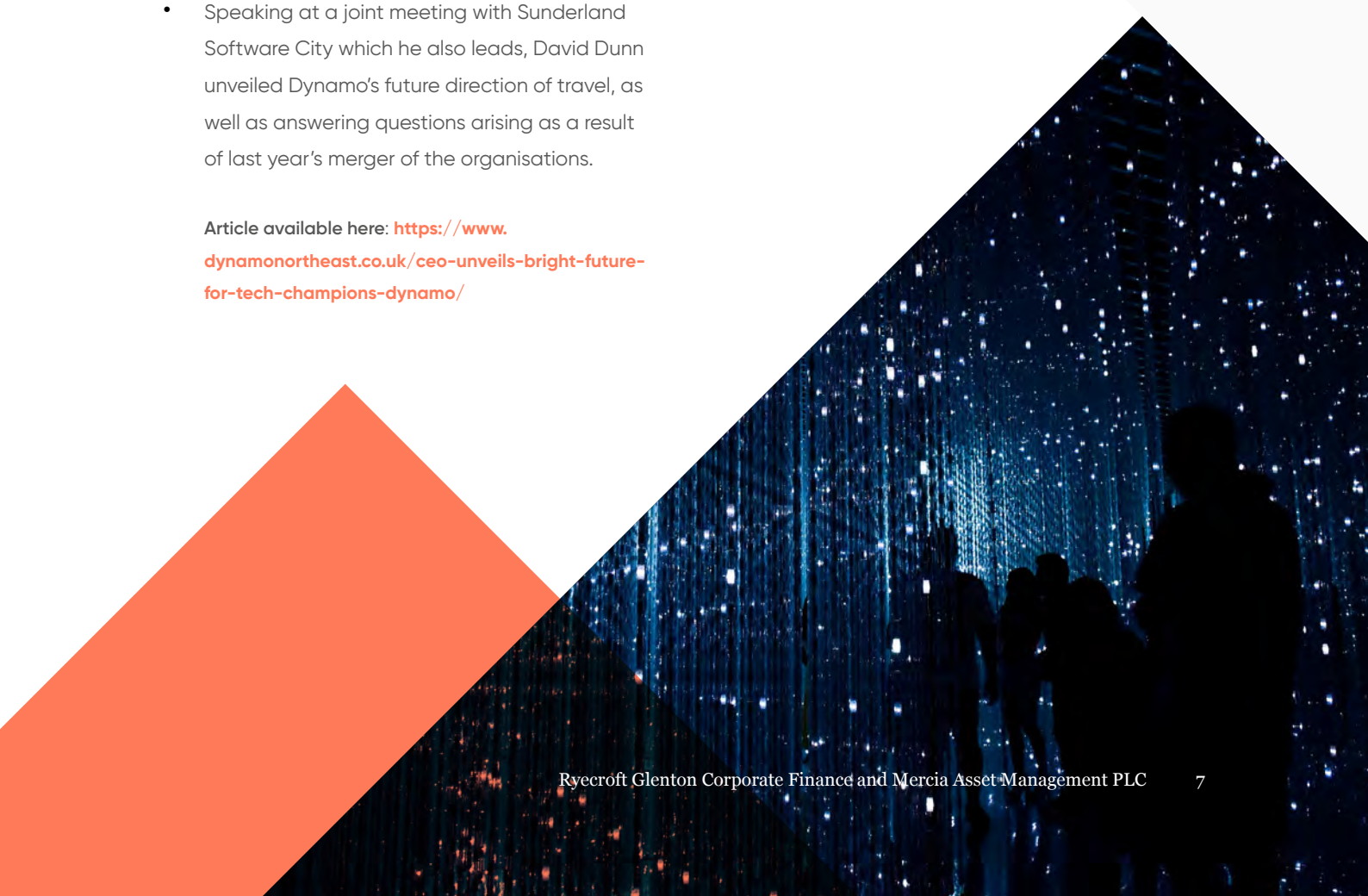
- The CEO of Dynamo has outlined his vision for a bright and ambitious future for the region's tech network.
- Speaking at a joint meeting with Sunderland Software City which he also leads, David Dunn unveiled Dynamo's future direction of travel, as well as answering questions arising as a result of last year's merger of the organisations.

Article available here: https://www.dynamonortheast.co.uk/ceo-unveils-bright-future-for-tech-champions-dynamo/

Maven invests £32.5m into North East tech in 2022

- Private equity firm Maven has said its North East division invested £15m in 2022 and secured an additional £17.5m in private sector finance.
- In the North East Maven provided financial support to 18 companies in sectors including tech, green energy, deep tech, manufacturing and support services.

Article available here: https://www.uktech.news/tech-hubs/the-north-of-england/maven-north-east-2022-20230214



Spotlight on the Cybersecurity sector

Cybersecurity is an increasingly important sector in a world that is becoming more and more connected. It is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cyber security measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organisation.

Cybersecurity protects against data breaches, which can be in the form of stolen or compromised credentials, phishing, cloud misconfiguration, and vulnerability in third-party software, as just a few examples. According to the IBM 2022 Cost of a Data Breach report, data breach costs increased by 13% between 2020 and 2022, the global average cost of a data breach is $4.35m, and it took an average of 277 days to identify a breach. Ransomware attacks are becoming more common, with the share of breaches being caused by ransomware increasing by 41% in 2022.[1]

This shows that as the digital economy grows, cyber security is going to get more and more important. At the current rate of growth, damage from cyber-attacks will amount to about $10.5 trillion annually by 2025, a 300% increase from 2015 levels.[2]

Based on all this, McKinsey has stated in a report that the gap today between the c.$150 billion vended market (the amount globally spent on cyber security in 2021) and a fully addressable market is huge. At approximately 10% penetration of security solutions today, the total opportunity amounts to a staggering c.$1.5 trillion to $2.0 trillion addressable market. This does not imply the market will reach such a size anytime soon (current growth rate is 12.4% annually of a base of approximately $150 billion in 2021), but rather that such a massive delta requires providers and investors to 'unlock' more impact with customers by better meeting the needs of underserved segments, continuously improving technology, and reducing complexity.[3]

Industry trends

Advances in artificial intelligence (AI) technology are allowing companies to respond to threats and breaches quicker. Companies that used AI and automation had a 74-day shorter breach lifecycle and saved on average $3m more than those without.[4] Providers of solutions will be striving to enable high-fidelity assisted intelligence to make human analysts more efficient, be it through leveraging advanced analytics or building tight integrations with other security platforms.

Integrating advanced technologies such as machine learning, artificial intelligence, big data analytics, and internet of things technology in cyber security solutions is expected to gain huge attention in the next five years. Also, the rapid adoption of cloud-based and analytics technology is putting businesses at risk. With the rise in investments and efforts to develop the telecommunication infrastructure and deployment of 5G technology, the frequency of cyber attacks is expected to grow. To combat such situations governments are promoting the adoption of cyber security solutions. Increased focus on developing advanced cyber security solutions and favourable government policies is expected to propel the UK's cyber security market in the next five years.[5]

Overview of Cybersecurity M&A

M&A activity within cybersecurity had been growing in recent years, but in 2022 the momentum dropped. There was a 14.6% decline in deal volume and a 56.7% decline in deal value when compared to 2021.[6] Given the large drop in value when compared to volume, this suggests an active market but that investors were increasingly cautious to commit big investments amid volatile market conditions.

In 2021, total M&A deal value was above $100 billion due to the announcement of big-ticket deals, such as the acquisition of McAfee for $14 billion by a consortium (composed of Advent International, Crosspoint Capital Partners, Permira Holdings, CPP, and GIC) and Thoma Bravo's acquisition of Proofpoint for $12.3 billion, among others. However, 2022 did not have announced deals valued at over $10 billion, hence the drop in deal value year on year. In 2022, global deal volume was over 400 for the fourth consecutive year.

1 https://www.ibm.com/reports/data-breach

2 Steve Morgan, "2022 Cybersecurity Almanac: 100 facts, figures, predictions, and statistics," Cybercrime Magazine, January 19, 2022.

3 https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar market-opportunity-for-cybersecurity-technology-and-service-providers

4 https://www.ibm.com/reports/data-breach

5 https://www.globenewswire.com/news-release/2023/02/10/2605911/0/en/United-Kingdom-Cyber-Security-Market-Report-2023-Increased-Complexity-of-Cyber-attacks-Drives-the-Market-Demand-Competition-Forecasts-Opportunities-to-2027.html

6 https://www.insurancebusinessmag.com/uk/news/cyber/report-looks-into-decline-in-cybersecurity-manda-activity-433150.aspx

Ones to watch

Melius Cyber is a cybersecurity business that has developed automated software to help SMEs detect vulnerabilities in their IT system. Mercia has invested in the business twice, with the latest round being £350k in July 2022. The business was founded in 2019 by Dave McPherson, a former IT specialist with the Bank of England. The company is a spin-off from Melius Group, the Newcastle-based IT services business he founded seven years earlier.

Netacea, which began life as a division of Intechnica in 2018, detects bot attacks that target mobile, web and API applications. It now employs a 100-strong team and supports some of the world's biggest brands including two of the top 10 global retailers and three of the world's largest telecommunications networks. Mercia invested as part of an £8.5m round in Intechnica in December 2021, Netacea was subsequently spun out of the company in July 2022. Mercia sold Intechnica earlier this year to US-based Crosslake Technologies but retains its shareholding in Netacea.

CyberHive has developed a patent-protected cyber security platform called Trusted Cloud – a cutting-edge technology, co-developed with the University of Oxford. Trusted Cloud uses a patented technique known as 'hardware-backed distributed whitelisting' to block cyber attacks and identify breaches in seconds that would go undetected by competing technologies for weeks or even months. Additionally, its 'Gatekeeper for Office 365' was designed to secure Microsoft Office 365 up to National Cyber Security Centre standards to protect remote workers from attack. Mercia invested in the business in 2021, with a £1.8m investment.

RG
RyecroftGlenton

mercia
asset management

The Changing Landscape of Cybersecurity

In 2022, the United Kingdom had the highest number of cybercrime victims per million internet users at 4,783 – a significant 40% increase over 2020. This number is not limited to simple phishing scams but includes large-scale supply chain disruptions and sophisticated hacking techniques.

As technology advances, supply networks are getting more integrated and complex. However, security flaws in one company can make connected partners vulnerable. Up to 40% of cyber threats now arise indirectly through the supply chain, and cybercriminals are taking advantage of these vulnerabilities.

Research shows that because of the rising demands of greater digital systems, cyber security professionals under pressure are struggling to cope effectively, leaving systems open to be exploited by cybercriminals. Furthermore, the interconnectedness of technologies between companies, and reliance on third-party support has led to vulnerabilities spreading across not just supply chains, but across different industries and world markets.

Companies such as Atlassian demonstrate the supply chain's hazards. With 180,000 clients worldwide, 83% of Fortune 500 organisations use Atlassian products. However, in June 2022, researchers revealed a serious flaw in Atlassian's technology. Thankfully, this flaw was discovered by researchers rather than attackers, allowing the company to make the necessary changes prior to an attack that could have had disastrous consequences for customers. According to the research, about 200,000 businesses may have been dependent on vulnerable organisations exposed to the risk of attack.

However, threats to cybersecurity are also becoming more widespread through our everyday devices, impacting consumers and users of technological devices, commonly referred to as the 'Internet of Things' ("IoT"). IoT attempts to create a broad and vast network of devices that are able to communicate succinctly, for example, cardiac rhythm monitoring in the home for greater health support, traffic management to alleviate congestion and air quality monitoring, sensors that track movement along the supply chain for efficiency, condition monitoring in agriculture or predictive maintenance and enhanced productivity to make manufacturing sleeker and scalable.

The IoT links different items and machines together so they can talk with other similarly connected machines or gadgets. Consumers can now buy a variety of things, from cars to refrigerators, using an online connection. We may become more effective, save time and money, and have access to our digital lives whenever we need it by expanding networking capabilities to every part of our lives. This enhanced connectivity, however, expands the attack surface, revealing a greater number of target points for attackers.

IoT device security is challenging for a number of reasons. Security is frequently accorded a lower priority than time-to-market metrics by manufacturers and innovators who are under pressure to deploy innovative goods. Also, a lot of firms are typically more focused on the cost reductions and convenience that IoT offers, and often neglect the vulnerabilities that IoT brings.

The stakes are particularly high for IoT systems used in the industrial sector. The operational hazards in anything from national power generation and distribution infrastructures to international industrial operations might be greatly increased by connected IoT sensors and devices.

Blockchain technology should be a key strategy when creating an IoT cybersecurity plan. Decentralised databases storing identical information simultaneously distribute information across thousands of 'nodes', massively improving resilience, and ensuring that any information stored is unable to be modified or removed. An attack on one or more nodes has no impact on the other nodes because each node is essentially any electronic device that keeps a copy of the blockchain. By limiting access to IoT devices by default, blockchain defends against data tampering and enables the shutdown of compromised devices in the network ecosystem without sacrificing the integrity of the data.

Sources:

https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=Global%20cyber%20crime%20statistics%3A,a%2013%25%20decrease%20over%202020

https://www.knowledgehut.com/blog/security/Iot-cyber-security

https://www.forbes.com/sites/forbestechcouncil/2022/06/16/cybersecurity-and-risk-management-in-the-internet-of-things/?sh=4d8d27663272

Zero trust

"Zero trust" has gained significant attention in the cybersecurity sector in recent years as a strategy to safeguard networks and boost security across businesses. The increasing popularity of this security paradigm can be linked in part to the shift to hybrid working habits, which require a more secure work environment whether on- or off-premises.

In contrast to the perimeter-based security approach, which presumes that anything originating within the corporate network is secure and trustworthy, zero trust assumes that no user or device can be trusted intrinsically - "never trust, always verify". This approach intends to safeguard modern settings and facilitate digital transformation by exploiting network segmentation and blocking lateral movement of devices on a network. However, zero trust remains an approach, rather than a set of rules to follow or products to purchase, and as such care must be taken to ensure that this approach is developed and maintained efficiently.

These principles, when paired with a set of best practices aimed at securing zero trust buy-in across the company as well as maintaining, monitoring, and improving the framework, can assist cyber leaders in ensuring that change does not disrupt the organization's business continuity.

While many businesses may already have some procedures and technologies in place for a successful zero-trust deployment, future trends should be considered. Artificial intelligence and biometrics, for example, can assist better in controlling cyber threats and contribute to the execution of the guiding zero trust principles. With so many factors to consider, it is no surprise that modern day cyber security approaches are more complex than ever.

To make matters worse, many organisations today operate with patchwork security solutions and poorly integrated tools. As a result, security teams are spending more time on manual tasks. They lack the context and insight needed to effectively reduce an organisation's attack surface. Increasing data breaches and tightening regulations worldwide are making it more difficult to secure networks, and the average cost of a data breach is increasing, currently costing approximately £3.3 million in business losses and fines.

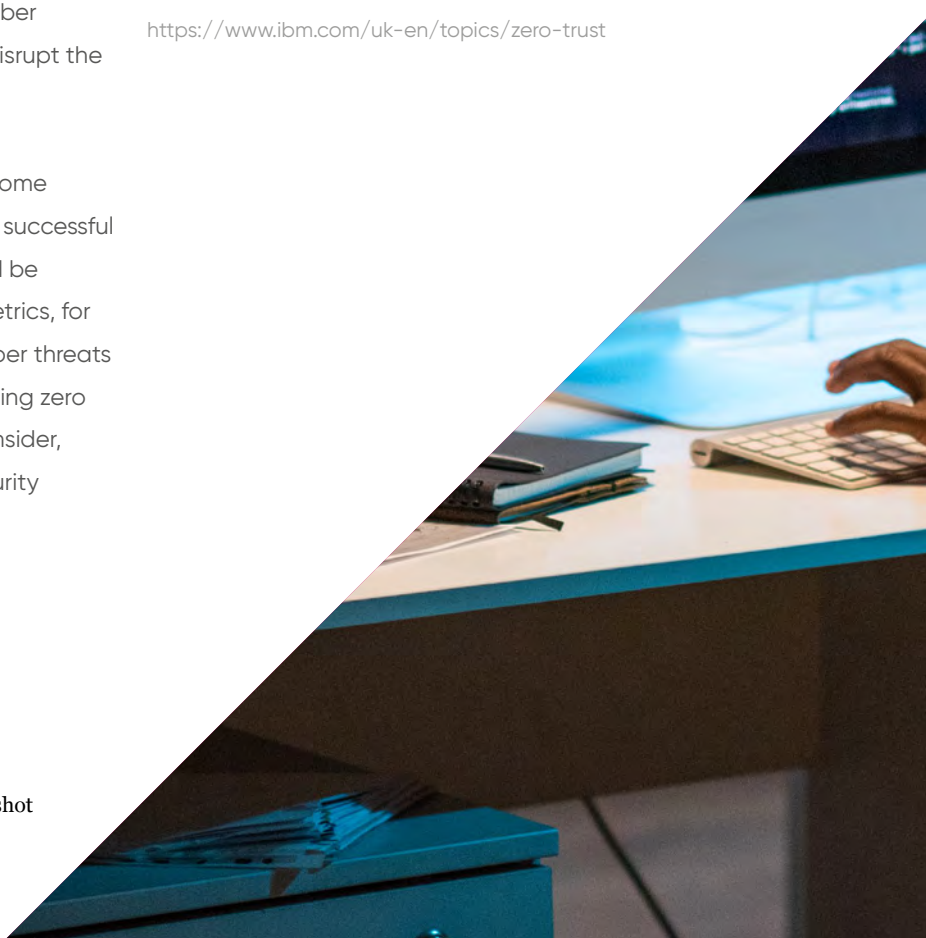
Zero trust is a long-term commitment that requires both financial and non-financial resources, as well as continuous prioritisation and support throughout the organisation, and it is therefore no silver bullet. However, with data breaches and other cyber attacks on the rise, an innovative approach such as a zero-trust system may provide an adequate response to a wide range of threats.

Sources:

https://www3.weforum.org/docs/WEF_The_Zero_Trust_Model_in_Cybersecurity_2022.pdf

https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

https://www.ibm.com/uk-en/topics/zero-trust




RG
RyecroftGlenton
mercia
asset management

RG in Discussion... about Cybersecurity

This quarter we've teamed up with Richard Brown, the CEO of North East based Melius Cyber. We asked him 10 quick-fire questions to learn more about his career and Melius. Richard has kindly agreed to be the guest speaker at our forthcoming seminar "How effective funding in the tech sector can unlock opportunities for growth" on 23rd March at Crowne Plaza Newcastle.

Find more information at the following link: **https://ryecroftglenton.com/events/**

RG: What is your background and how has that led you to Melius?

Richard: I'm a Chartered Accountant, I started my career at Price Waterhouse in Manchester and went into the Corporate Finance Team there for a few years, prior to working for a couple of Corporate Finance Boutiques. I then worked in industry and also set up and ran a couple of non-tech businesses. The Melius opportunity came through one of the other founders. He has the cyber and tech skills whilst I bring the finance, management and business structure.

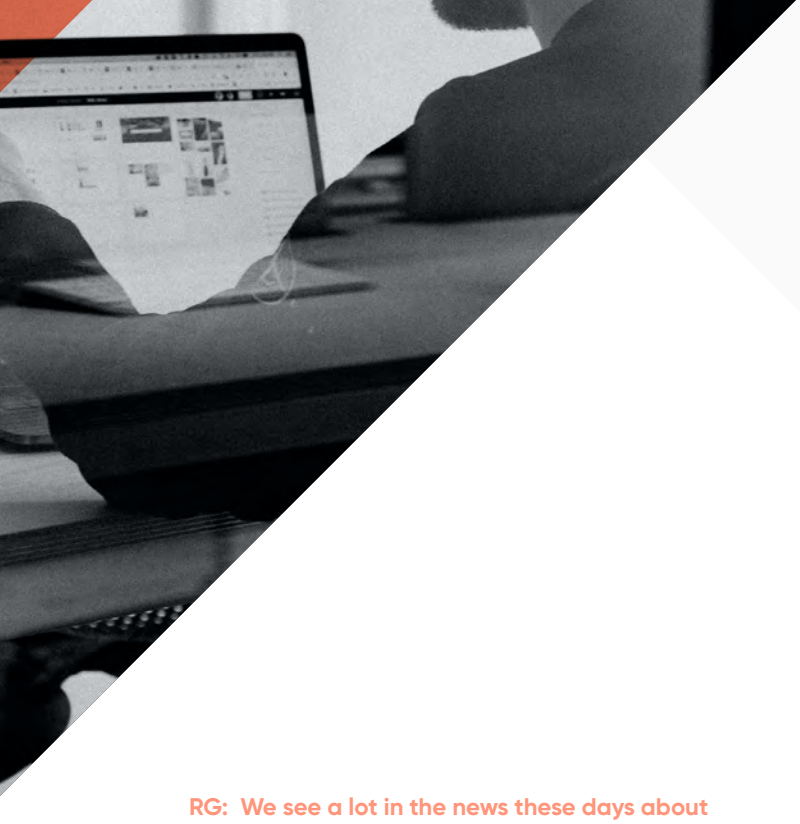
RG: What does Melius do?

Richard: In short, we provide a plug-in cyber security solution for the SME market. This is a 24/7 vulnerability scanning and penetration testing tool which takes a number of products and in-house software to scan a business's entire IT estate for threats, it also carries out Phishing attacks and other behavioural testing for the workforce. The threats and vulnerabilities are displayed on a user-friendly dashboard with plain English explanations. This allows our clients to see and react to issues, they may fix them internally, seek assistance from us or revert to their existing support company to resolve them.

In addition, we can prepare and certify clients for Cyber Essentials & Cyber Essentials Plus, and we provide penetration testing services.

RG: What makes Melius special?

Richard: We are focused on the SME market and making cyber security accessible and simple for all. We are a service that really supports customers in a personable way, not just a boxed product that you instal and hope for the best.



RG: We see a lot in the news these days about cyber-attacks, ransomware, attacks from hostile states etc. How much of this do you see on a daily basis?

Richard: Most breaches go under the radar and are from automated bots that test for weaknesses. This means smaller organisations are more vulnerable because they don't have the resources to protect themselves. Full-scale denial of service/ransomware is still a rarity in the SME market, but it does occur. All data has value, and cyber-attacks are virtually anonymous. Ransomware is usually demanded in cryptocurrency and as such is untraceable, so unfortunately it is a massively growing area of crime. All businesses are under threat because none of us can work without access to our data or systems.

RG: What is the best way to make sure a business is protected?

Richard: Be preventative, not reactive; our system tests for over 200,000 threats every day and the list is constantly growing. These attacks happen as a result of a breach, and our aim is to prevent breaches. The latest statistics from IBM show that the average time taken to detect a breach is 277 days with a further 69 days to contain it. Indeed, many breaches lie undetected for months leaving businesses open to attack: our system will detect a breach within 24 hours. Ultimately, the best way to minimise risk is through regular testing and proactive management of your environment and cyber risk profile.

RG: How does the industry stay proactive to risks, as opposed to reacting to a new type of cyber-attack?

Richard: Large organisations have the resources and skills to protect themselves and use a variety of 3rd parties to test that they have the correct measures in place. This is just cyber security best practice and is often referred to as 'not marking your own homework'. Usually in the form of a consultant, ethical hacker, penetration tester or a cyber security auditor. Our Cyber Safe product was built to automate what these 3rd parties do, at a fraction of the cost and specifically for SMEs.

RG: What advice would you give to somebody who thinks their business is safe because it's in a certain industry or a certain size?

Richard: Be proactive, don't just accept the status quo, challenge your IT provider on these issues and seek specialist advice. Cyber security is not anti-virus, firewalls and passwords: it is much more than that.

RG: How far has the sector advanced, and is it advancing quickly enough to match the sophistication of the risks arising?

Richard: The sector is very advanced and at the top level there is massive investment in security for example the National Cyber Security Centre and the US Cybersecurity & Infrastructure Security Agency work to contain, mitigate and educate around the clock. Larger companies take it very seriously (due to the threat of fines, loss of revenue, reputational damage etc.). However, the threat environment expands daily and the sector needs to attract more skilled staff. At Melius, we have focused on recruiting Graduates from the local Universities and training them towards the gold standard industry accreditations.

RG: How has AI changed the industry?

Richard: This is an interesting area that we are looking at developing further into. Machine Learning can assist in testing and exploitation of vulnerabilities along with increased automation of testing. However, thought leadership and the changing geopolitical environment is a key driver for cyber threats which are perhaps beyond their current limitations.

RG: What do you expect from the industry within the next 5 years?

Richard: There will continue to be an increase in the amount of sophistication of cyber-attacks which will use tools not yet invented. I suspect there will undoubtedly be some high-profile attacks with some eye-watering ransoms. We expect attackers will move even more to exploit smaller businesses because they lack the investment in defence. It is therefore important that the industry continues to invest and retain and train top talent.


RG
RyecroftGlenton
mercia
asset management

Some Interesting Deals in the UK Technology Sector

(Oct-22 to Dec-22)

The deals that have been selected below have been chosen to show the variety and diversity of activity in the sector in terms of deal types and sub-sectors.

Date: Closed	Target	Acquirer / Funder	Sub Sector	Target Product Line	Value / Investment funding	Region	Deal Type
11-Oct-2022	Community Fibre	Ischyros New York	Communications and Networking	Operator of a broadband company primarily intended to serve the residents and businesses across London.	£985m	London	Debt - General
19-Oct-2022	Arqiva	Digital 9 Infrastructure	Communications and Networking	Operator of a communications infrastructure company intended for terrestrial network transmission as well as television and radio broadcast.	£909m	Winchester	Secondary Transaction - Private
07-Dec-2022	Curve	Credit Suisse	Software	Developer of a banking platform intended to consolidate multiple cards and accounts into one smart card and application.	£840m	London	Debt - General
01-Dec-2022	Quantile	London Stock Exchange Group	Software	Developer of a counterparty risk optimization platform.	£274m	London	Merger/ Acquisition
11-Oct-2022	Lending Works	BNP Paribas (PAR: BNP)	Other Financial Services	Operator of a peer-to-peer lending platform.	£200m	London	Debt - General
13-Dec-2022	NoviCap	Fasanara Capital	Software	Provider of an online invoice trading marketplace.	£173m	London	Debt - General
01-Dec-2022	Pay360	Access PaySuite	Other Financial Services	Provider of online payment services based in London.	£156m	London	Merger/ Acquisition
12-Dec-2022	Zappi	Sumeru Equity Partners	Software	Developer of automated market research platform.	£139m	London	PE Growth/ Expansion
14-Dec-2022	PragmatIC	Amcor, British Patient Capital, In-Q-Tel, Maven Capital Partners UK, among others	Semiconductors	Developer of a circuit technology designed to provide low-cost flexible integrated circuits.	£130m	Cambridge	Later Stage VC
19-Dec-2022	Updraft	Auluk Investments, Faber Capital, LC Nueva Investment Partners	Software	Developer of a financial platform designed to help people pay off existing credit.	£108m	London	Later Stage VC

Date: Closed	Target	Acquirer / Funder	Sub Sector	Target Product Line	Value / Investment funding	Region	Deal Type
10-Oct-2022	Connex One	GP Bullhound	Software	Developer of a customer engagement platform that is designed to enable inbound and outbound interactions.	£93m	Manchester	PE Growth/ Expansion
05-Oct-2022	Stability.AI	Coatue Management, Fourth Revolution Capital, Lightspeed Venture Partners, Mantis VC, among others	Software	Developer of an open AI tool designed to create images based on text input given.	£89m	London	Early-Stage VC
10-Oct-2022	Global Connectivity	Tiger Infrastructure Partners	Communications and Networking	Prioritisation high-speed connectivity within rural communities through the implementation of hybrid infrastructure.	£75m	Douglas	PIPE
12-Oct-2022	Bud	Banco de Sabadell, Investec, SEI Investments, Stanley Fink, TDR Capital	Software	Developer of an open banking application.	£72m	London	Later Stage VC
14-Oct-2022	Blockchain.com	Ash Park Capital, Fort Ross Ventures, Human Capital, Kingsway Capital	Software	Developer of a digital assets platform.	£70m	London	Later Stage VC
06-Dec-2022	Attraqt Group	K1 Investment Management	Software	Engaged in the development and provision of eCommerce site search.	£63m	London	Buyout/LBO
09-Nov-2022	Ramp Network	Cogito, Cogito Capital Partners, Mubadala Capital-Ventures, among others	Software	Operator of a financial technology company intended to build payment rails connecting crypto to the global financial system.	£61m	London	Later Stage VC
12-Oct-2022	Immersive Labs	Ten Eleven Ventures	Software	Developer of a human cyber readiness platform.	£59m	Bristol	Later Stage VC
25-Oct-2022	What3words	Alain Garner, German Media Pool, Hippolyte Genêt, Monday Capital (Accelerator), Niya Partners, among others	Media	Developer of a mobile-based location platform.	£58m	London	Later Stage VC
19-Dec-2022	Moneyhub	Shawbrook Bank	Software	Developer of an open finance platform designed to help understand and engage with customers.	£55m	Bristol	Later Stage VC

Source - Pitchbook

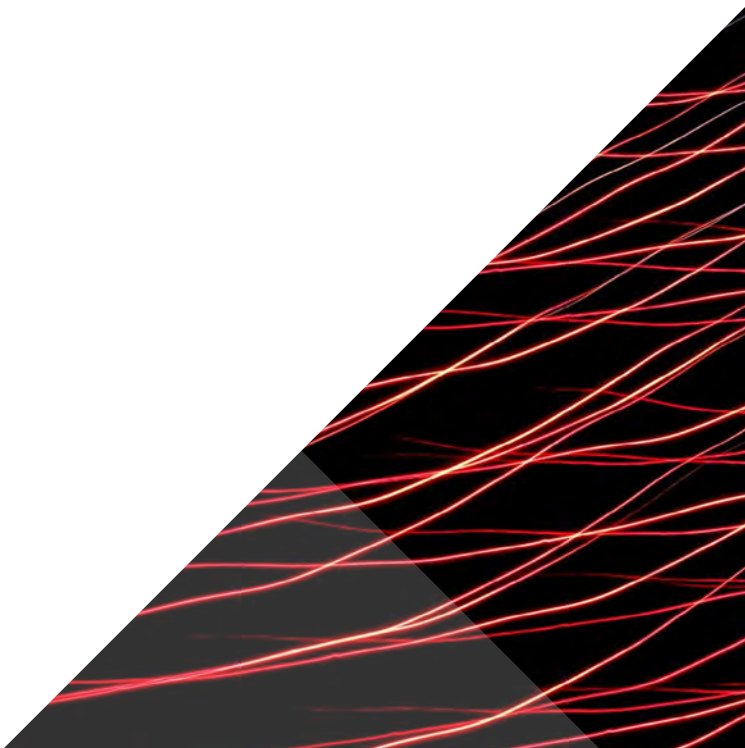
Some Interesting Deals in the North East Technology Sector

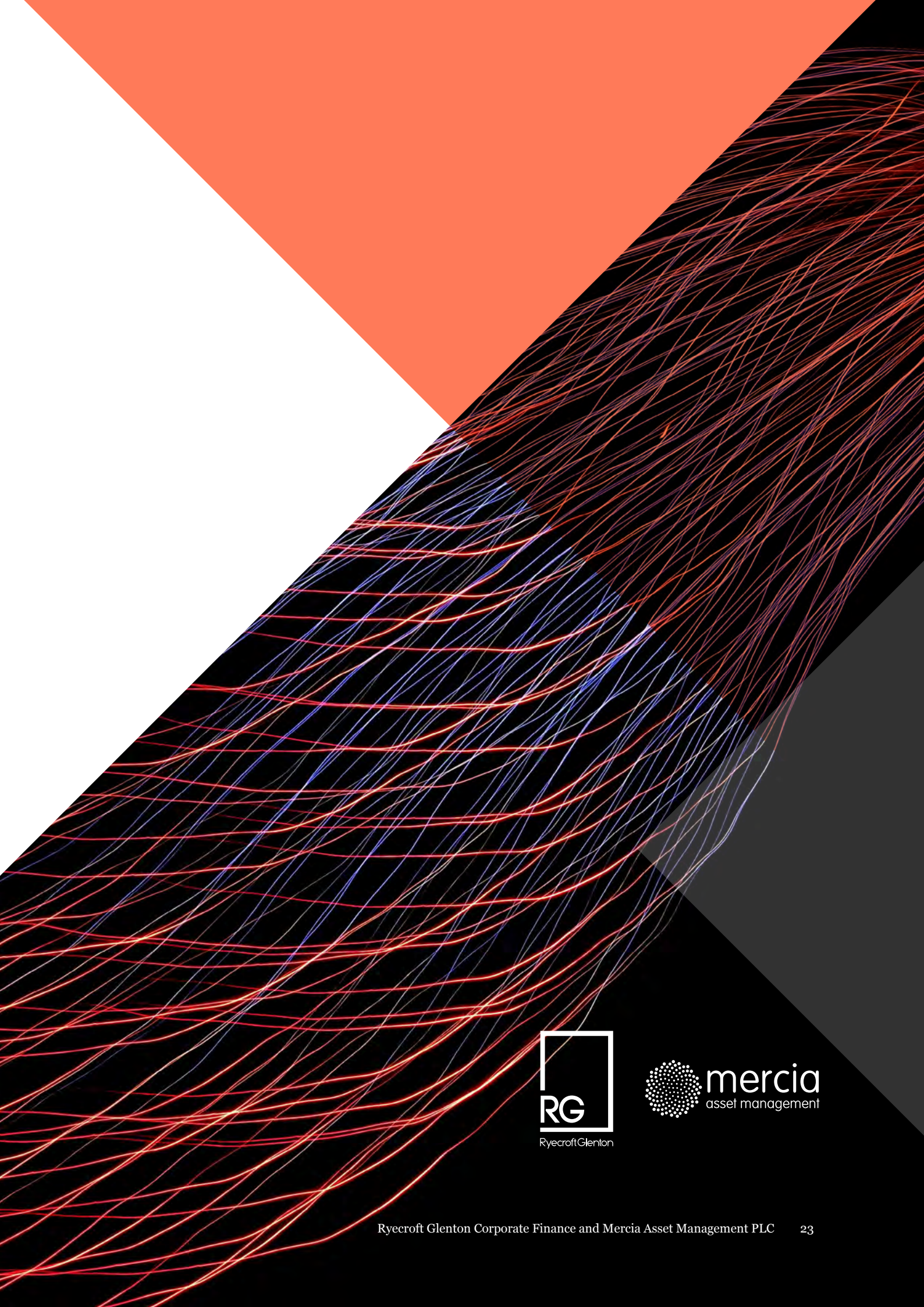
(Oct-22 to Dec-22)

The deals that have been selected below have been chosen to show the variety and diversity of activity in the sector in terms of deal types and sub sectors.

Date: Closed	Target	Acquirer / Funder	Sub Sector	Target Product Line	Value / Investment funding	Region	Deal Type
03-Nov-2022	Audemic	Startup Wise Guys	AudioTech, EdTech	Developer of an E-Learning application	£900k	Durham	Accelerator/ Incubator
28-Nov-2022	Protector Group	Argenbright Group	Robotics and Drones	Developer of security products and services	N/D	Gateshead	Merger/ Acquisition
22-Nov-2022	Reading Solutions UK	Mr Ian Fitzpatrick (MBO)	Educational and Training Services	Provider of education services	N/D	Gateshead	Merger/ Acquisition
04-Oct-2022	REALRIDER	Rivers Capital Partners	Mobile, SaaS	Developer of an online smartphone technology	N/D	Gateshead	Secondary Transaction - Private
04-Oct-2022	Venture Stream	Rivers Capital Partners	Marketing Tech, SaaS, TMT	Provider of online digital marketing services	N/D	Newcastle Upon Tyne	Secondary Transaction - Private

Source - Pitchbook




RG
RyecroftGlenton
mercia
asset management

A Closer Look at Some Notable Technology Deals Supported by RGCF and Mercia

Turbine Simulated Cell Technologies

In November 2022, Mercia invested £4.5m from the Northern VCTs into Turbine Simulated Cell Technologies as part of a €19.0m round, which was co-led by Mercia and Merck's CVC arm. Other investors in the round include Accel, XTX, Delin Ventures, Day One Capital.

The company was founded in 2015 and is a spin-out of the Technical University of Budapest. Turbine has created a computer model of the inner workings of cancer cells, allowing it to run simulations far faster and cheaper than conventional methods to understand the biology and potential impact of cancer treatments. The company can run millions of simulations a week to identify novel cancer therapies, discover biomarkers that can be used to stratify populations for improved chance of successful clinical trials, predict the efficacy of cancer drug combinations and find new applications for existing drugs, thus increasing patent timelines.

Huler Group

In December, Mercia invested £2.0m into Huler Group. Huler is an employee experience platform ('EXP') that provides a front-end wrapper to various internal systems (Internal Comms, Learning Management Systems, Workflow Management, Employee Engagement Surveys, Slack, etc.). Huler combines the use case of a traditional intranet system with the UX / UI of a Netflix or Prime.

HowNow

Mercia invested £3.0m as part of a £4.0m Series A round into London-based HowNow in January. This was a syndicated investment alongside Pearson Ventures, the corporate venture arm of Pearson Plc.

HowNow is a Learning Experience Platform - a new, fast-growing category within the Learning Management Systems market typically characterised by on-demand, self-directed and peer-to-peer learning. HowNow's platform tries to solve the problem of context in corporate learning. Its product consists of a traditional learning management system (LMS) where customers can host their learning content and an experience layer with the ability to: 1) dynamically map employees to relevant content, and 2) surface up learning content in the flow of work when the employee is looking for information outside the company's LMS.

Slingshot Simulations

In January, Mercia led a £3.0m funding round into Leeds-based Slingshot Simulations. Mercia invested £1.5m, with Northern Gritstone investing the other £1.5m.

Slingshot has developed a low-code decision intelligence platform which provides users with a faster way to integrate, visualise, analyse and simulate data. The use of digital twins to test and predict scenarios to optimise processes is a rapidly growing market and one which Slingshot has been focused on since its founder, David McKee spun the business out from Leeds University in 2019.

Market Dojo

Esker, a global cloud platform provider and leader in AI-driven process automation solutions announced in January 2022 that it plans to acquire 50.1% of Market Dojo. The transaction is due to complete in 2022.

Based in Bristol, Market Dojo has 20 employees and over 160 customers, 60% of which are outside its domestic market, including France, the United States and the Middle East. Market Dojo's eSourcing cloud solution was created to address the need for structured and digitised processes in procurement. Designed by procurement professionals, Market Dojo's unique on-demand solution enables users to centralise information, negotiate the best value for goods and services and select the right suppliers — all without requiring a complex and costly implementation process.

Ryecroft Glenton Corporate Finance advised Market Dojo on the sale of their business to Esker.

Send Technology Solutions

Mercia invested £3m into Send Technology Solutions in November 2022, as part of a £9m round led by Breega. Send provides underwriting workbench software to insurers, re-insurers and Managing General Agents on large enterprise contracts, enabling underwriters to save as much as 40% of their time by organising all their data into a single system.

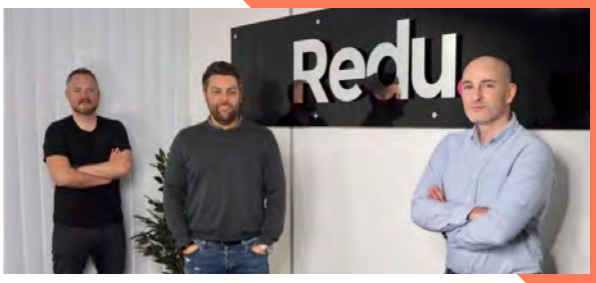
To date, the business has been bootstrapped, growing to £8m turnover in 2022 with annual recurring revenue (ARR) growth over 175% for the last two years

VTUK

VTUK, a cloud-based property CRM software platform has been acquired by The iamproperty group for an undisclosed sum.

Established in 1989 by founder Peter Grant, it works with more than 300 estate agencies across the UK and already shares a number of mutual customers with iamproperty. VTUK offers functionality-rich CRM solutions including Openview, a cloud-based property CRM software platform. The platform creates a seamless and intuitive experience that enables agents to fully automate their day-to-day operations.

Ryecroft Glenton Corporate Finance advised the shareholders of VTUK on the sale of the business to iamproperty.



Redu Group / MBL Solutions

MBL Solutions, a North East gift card provider has been acquired from Redu Group by Appreciate Group for an undisclosed fee. Appreciate is known for owning such names as Love2shop, Park Christmas Savings and highstreetvouchers.com.

MBL Solutions was previously acquired by Redu Group during the pandemic, which saw the team grow the business over the next 18 months, increasing turnover and headcount, whilst bringing significant clients on board and providing further solutions to the market.

Ryecroft Glenton Corporate Finance advised Redu Group on its disposal of MBL Solutions.

Authors

Nick Johnson

Nick is a partner within RG Corporate Finance, advising businesses on all aspects of growth, change and transformation. Nick leads RG's technology team.

0191 2125915
nickjohnson@ryecroftglenton.com

Benjamin Kain

Ben is an Corporate Finance Executive within the RG Corporate Finance team working on a wide range of CF transactions. Ben is also a member of RG's technology team.

0191 212 5922
benkain@ryecroftglenton.com

Harry Lamb

Harry is a Tax Assistant working within the RG Business Tax team, and is involved in projects across the spectrum from R&D claims to share planning. Harry is also a member of RG's technology team.

harrylamb@ryecroftglenton.com

Ian Wilson

Ian is the Fund Principal for the North East Venture Fund and, in addition to acting as a member of Mercia's Investment Committee, is focused on early-stage and technology investments across the North East.

0191 731 4130

Ian.Wilson@mercia.co.uk

Alex Simpson

Alex is a Investment Manager for the North East Venture Fund and is responsible for sourcing and executing early-stage and technology investments deals in addition to portfolio management.

0191 731 4133

Alex.Simpson@mercia.co.uk

North East: M&A Technology Sector Snapshot is a joint production from Ryecroft Glenton Corporate Finance and Mercia Asset Management PLC.

Deals

Smart Energy Technology

Provision of Corporate Finance advice and financial and tax due diligence services to Shard Credit Partners on its investment in the Management Buyout (MBO) of Chameleon Technology (UK) Ltd.

Procurement Technologies

Provision of Corporate Finance advice to the shareholders of Market Dojo Limited on the sale of 50.1% of the business to Esker Inc., a technology company listed on the Paris Stock Exchange

Unified Telecommunications

Provision of Corporate Finance advice to the shareholders of Nice Network Ltd on the sale of the business to LDC backed Onecom Group.

Ed-Tech

Provision of Corporate Finance advice to the management team of e-Quality Solutions Group on their MBO of the business, in a deal funded by Shard Credit Partners.

Technology

Provision of Corporate Finance advice to the shareholders of Vision Teknology UK Ltd on the sale of the Business to iamproperty Group, backed by LDC

Technology

Provision of Corporate Finance advice to Redu Group, on their disposal of MBL Solutions, a North East based gift card and reward provider to Appreciate Group, a publicly listed gift card and reward product provider.

Employee Welbeing

Provision of Corporate Finance advice to Latus Health Limited on the acquisition of Reward Me Now.

Art Health Solutions

arthealthsolutions.com

£800k equity investment from Mercia

Gateshead

Little Journey

littlejourney.health

£1.4m equity investment from Mercia

London

Broker Insights

brokerinsights.com

£4.1m equity investment from Mercia

Dundee

RG
RyecroftGlenton

mercia
asset management