Company Note

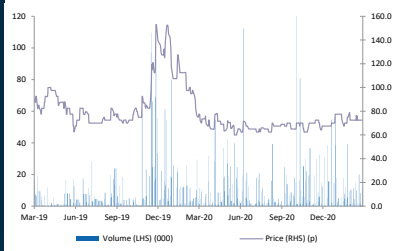
Finals

24 March 2021

Corporate

Current price	**75.0p**
Sector	**TMT**
Code	**ECSC.L**
AIM	**AIM**

Share Performance



	1m	3m	12m
ECSC.L	+5%	+13%	+1%

Source: Thomson Reuters, Allenby Capital

Share Data		
Market Cap (£m)		**7.5**
Shares in issue (m)		**10.0**
52 weeks	High	Low
	79p	**60p**
Financial year end		**31 December**

Source: Company Data, Allenby Capital

Key Shareholders	
Ian Mann	22.99%
Unicorn Asset Management	14.48%
Ravinder Bahra	10.68%
Hargreaves Lansdown	5.16%
Phil Mclear	4.72%

Source: Company Data, Allenby Capital

David Johnson

0203 394 2977

d.johnson@allenbycapital.com

www.allenbycapital.com

ECSC Group plc (ECSC.L)

Growth in MDR; recovery in Assurance

FY20 results in line with January's trading update for the UK's longest-running 'full service' cyber security provider with revenue growth in H2 over H1 and EBITDA accelerating during the year. The first lockdown impacted Q2 Assurance activity as consultants were unable to go onsite but this has since recovered. Meanwhile Managed Detection & Response (MD&R) continued to grow. As remote working has become the new norm, cyberattacks have proliferated and cyber security has moved back up the agenda with high-profile incidents and associated fines focussing attention. ECSC remains well positioned to capitalise on the opportunity via direct sales and its established partner network. It has proven expertise and high staff retention, backed by its proprietary technology stack. We reintroduce forecasts that show a return to revenue growth but also targeted recruitment that will depress FY21 EBITDA before accelerating. We set a fair value of 130p/share, equivalent to a FY22 EV/EBITDA of 21.0x.

- **FY20 performance:** FY20 revenue fell 4.1% to £5.7m (FY19: £5.9m), reflecting the impact of COVID-19 on the Assurance division in Q2 as well as lower client chargeable expenses. Assurance revenue fell 6.8% to £2.7m. MDR revenue increased 5.7% to £2.7m and MDR recurring revenue by 22% to £2.4m. There was a good recovery in Assurance since the Q2 lockdown where revenue fell 50% on Q2 FY19. Q3 was down only 4% and Q4 saw 6% growth. Overall, 90 new clients were secured (FY19: 118). Adj. EBITDA of £0.4m (FY19: breakeven) indicates H2 profit of £0.3m, reflecting H2 revenue growth and ongoing cost control. FY20 cash of £1.1m (FY19: £0.4m), includes £0.4m of COVID-19 related medium-term government support. The Group's £0.5m bank facility remains unutilised.

- **COVID-19 response:** Management navigated the challenges posed by COVID-19 well and responded rapidly: re-engineered services to enable remote/home working; ensured the uninterrupted delivery of 24/7 managed services; strengthened the balance sheet; made use of government support schemes; and reduced the cost base to remain at least break even during the Q2 revenue dip that management estimates at £0.4m (Assurance and recharged client expenses). At the same time, ECSC continued to invest in its AI technology base (equivalent to 14% of revenue). This stack is a key differentiator, supporting its experienced team of cyber security professionals and enabling scaled growth.

- **Outlook:** FY21 has started well with major MDR contract wins with a major UK charity and a national leisure group and ECSC is positioned to capitalise on the growth opportunities in the UK cyber security market as outsourcing remains the logical choice for all but the largest organisations. FY21 forecasts show revenue growth plus investment in headcount that boosts profits in FY22. Our fair value of 130p/share is equivalent to an FY22 EV/revenue of 1.5x and EV/EBITDA of 21.0x.

Year End: 31 December					
(£'000)	**2018A**	**2019A**	**2020A**	**2021E**	**2022E**
REVENUE	5,382	5,905	5,663	6,563	7,898
ADJ. EBITDA	(635)	1	375	153	564
ADJ. PBT	(1,026)	(639)	(153)	(411)	(0)
ADJ. EPS (p)	(10.5)	(6.8)	(0.9)	(3.8)	(0.0)
NET CASH	610	351	1,122	1,092	1,176
EV/EBITDA (x)	NEG	>100	17.0	41.9	11.2
PER (x)	NEG	NEG	NEG	NEG	NEG

Allenby Capital acts as Nomad & Broker to ECSC Group plc (ECSC.L).

Investment summary

ECSC Group plc provides investors with exposure to the growing cyber security services market through its two divisions: Managed Detection and Response (MDR) and Assurance. MDR covers managed services (monitoring and alerting) and incident response and Assurance involves services around penetration testing, standards and certifications.

Longest-running full service cyber security provider

ECSC represents the UK's longest-running full service cyber security provider with more than twenty years' experience. Over this time, it has built its own proprietary technology stack to support its Security Operations Centres (SOCs) in the UK and Australia. The systems are designed to cover multiple clients from a single interface and the IP includes the KEPLER AI system that sifts through vast quantities of data logs to identify potential incidents that require further human investigation. ECSC continues to invest in its IP, spending c. 14% of revenue per annum. The company also enjoys the lowest staff attrition rates in a sector that has consistently struggled with staff retention (91% retention in 2020).

Partner Programme

ECSC has a broad base of customers across multiple sectors with no major revenue concentration – in FY20 the largest customer accounted for c. 5% of revenue – and counts 10% of the FTSE 100 as clients. It operates predominantly in the UK but has done work in more than thirty countries. The company also has a long history of organic growth, typically averaging 20% per annum. Although it will look at acquisitions, management does not believe that acquisitions are necessary to fuel future growth. In 2019, it initiated a Partner Programme that enables it to expand its addressable market, particularly into SMEs that typically have a trusted IT supplier, and more than 150 partners are now signed up and this channel contributed 4% of revenue.

Core areas of focus

Core areas of focus are the further development of the Partner Programme; ongoing development of the technology stack; and increasing market share, particularly through the upselling Assurance customers with MDR agreements. These MDR contracts provide greater revenue visibility and represent a much more scalable model as they leverage off ECSC's SOCs and its AI technology. Increased SOC utilisation drives margin appreciation at the divisional and group level.

Cyber security breach detection and expert incident response is vital to the protection of personal information and the maintenance of critical IT systems and needs to be carried out on a 24/7/365 basis. Outsourcing these critical functions is the logical choice for all but the largest global organisations as it is the only cost-effective solution. Clients also benefit from the service provider's much broader view of the threats posed to an organisation.

High-profile hacks

High-profile hacks, such as Solarwinds, highlights the persistent and pervasive threat faced by all companies and countries. And the increasing volume of large fines levied against companies for failing to protect client data (e.g. British Airways, Marriott Hotels and Ticketmaster) is focusing the attention of boards.

The UK cyber security market is reported to be worth more than £8bn per annum according to UK Government analysis last year and is growing at 9% per annum (Source: Plimsoll Report 2020). The proliferation of breaches is making cyber security a strategic governance issue for company boards and the UK GDPR legislation is in force that makes immediate breach reporting mandatory and fines of up to 2% of global revenue.

Current year has started well

ECSC successfully navigated the challenges posed by COVID-19 during 2020. The current year has started well with contracts in both Assurance and MDR via direct and indirect sales channels and we anticipate a return to revenue growth in FY21. ECSC has also resumed recruitment, following the hiatus in 2020. This investment, coupled with a lower

anticipated R&D tax credit, is likely to result in a lower FY21 adj. EBITDA before rebounding in FY22.

Fair value of 130p/share

The current share price fails to reflect ECSC's considerable experience and expertise in the cyber security sector, its history of growth (before the 2020 blip) and the value of its technology stack that enables the company to scale rapidly. We set a fair value of 130p/share is equivalent to an FY22 EV/revenue of 1.5x and an EV/EBITDA of 21.0x.

Although this represents a significant upside to the current price, the fair value multiple remains modest compared to many others in the cyber security space, particularly given the investment made in its technology offering. For example, NCC (NCC.L) is currently on an FY22 EV/Revenue of 2.7x. Meanwhile many of the other listed cybersecurity players with an investment in IP remain loss-making. As ECSC demonstrates its return to growth and margin appreciation through greater SOC utilisation, we would expect the multiple would increase.

FY20 financial and operational performance

Exhibit 1: Summary FY20 performance

	FY19	FY20	% change
Revenue			
Assurance	2,922	2,724	-6.8%
MDR	2,585	2,732	+5.7%
Vendor Products	162	125	-22.8%
Other	236	82	-65.3%
	5,905	**5,663**	**-4.1%**
Gross Margin			
Assurance	53.9%	57.9%	+4.0ppts
MDR	67.5%	73.0%	+5.5ppts
Vendor Products	17.9%	20.0%	+2.1ppts
Other	5.1%	-57.3%	NA
Gross profit	**3,360**	**3,548**	**+5.6%**
Gross margin	**56.9%**	**62.7%**	**+5.8ppts**
Adjusted EBITDA*			
Other Income	263	297	+31.9%
Sales & Marketing Costs	-1,958	-1,713	-12.5%
Administration Expenses	-1,664	-1,757	+5.6%
Adj. EBITDA	**1**	**375**	**>100%**
EBITDA			
Share Based Payments	-105	-101	-3.8%
Exceptional Items	-6	-65	>100%
EBITDA	**-110**	**209**	**NA**
Cash	**351**	**1,122**	**>100%**

Source: Company; Allenby Capital * excludes one-off charges and share-based charges

Group revenue fell 4.1% to £5.7m (FY19: £5.9m), reflecting the impact of COVID-19 on the Assurance division as well as client chargeable expenses (Other) in Q2. This indicates revenue growth in H2 over H1 (£3.0m versus £2.7m), although H2 revenue was down c. 10% on H2 FY19, reflecting some impact of COVID-19 continuing into Q3.

Assurance – Q2 disruption

Assurance revenue fell 6.8% to £2.7m but there was a good recovery following the Q2 lockdown where revenue fell 50% on Q2 FY19 with Q3 down only 4% and Q4 up by 6%. 90 new clients were secured in FY20 (FY19: 118). This is important not only as a revenue stream but Assurance clients also represent the main source of MDR clients. Gross margin returned to historic levels (58%) following the Brexit-related dip in FY19 (54%).

MDR – growth in recurring revenue

MDR revenue increased 5.7% to £2.7m and MDR recurring revenue by 22% to £2.4m. H1 was notable for a lower level of higher margin incident response work but this is now

picking up. The MDR order book remained flat at £2.6m as clients tended towards shorter managed service contracts and renewals given the general economic uncertainty. Increased utilisation resulted in a further 5ppts increase in gross margin (73%).

Exhibit 2: Key performance indicators

	FY18	FY19	FY20
Revenue growth	35.0%	10.0%	-4.0%
Managed Detection & Response Recurring Revenue Growth	46.0%	27.0%	22.0%
Managed Detection & Response Recurring Revenue Proportion	29.0%	34.0%	43.0%
Managed Detection & Response Order Book (£m)	2.5	2.6	2.6
Managed Detection & Response Gross Margin	53.0%	68.0%	73.0%
Assurance Repeat Revenue	78.0%	73.0%	73.0%
Assurance Gross Margin	57.0%	54.0%	58.0%
Research and development (of revenue)	8.5%	13.0%	14.0%

Source: Company; Allenby Capital

Group gross margin benefited from the change in revenue mix, increasing 5.8ppts to 62.7%. Adj. EBITDA of £0.4m (FY19: breakeven) indicates H2 profit of £0.3m, reflecting H2 revenue growth and ongoing cost control.

Good working capital management

ECSC maintained good cash collection during the pandemic with working capital essentially flat and very low levels of bad debt (<£10k). Cash generated from operating activities (£377k) was equivalent to 100% of adj. EBITDA. Capex was minimal but the company maintained capitalised development spend at £194k. FY20 cash of £1.1m (FY19: £0.4m), includes £0.4m of COVID-19 related medium-term government support, as well as April's £0.5m (gross) placing. The Group's £0.5m bank facility remains unutilised.

Operational highlights

COVID-19 response

ECSC moved quickly in response to the pandemic to mitigate in four areas: re-engineering all services to be delivered remotely; reductions made to the cost base and delivery capacity; strengthening the balance sheet with April's £0.5m placing (gross); and making use of UK and Australian support schemes where appropriate.

Monthly webinars

ECSC has changed its sales and marketing programmes with the switch to monthly webinars from quarterly physical events with the onset of COVID-19 restrictions. These webinars have proved to be successful with much higher numbers of attendees and management reported that more than two thirds of attendees are non-clients. The webinar model is also much more cost and time effective.

MDR contracts

In November, ECSC announced MDR contracts worth an aggregate £580k over three years secured with a major UK rail company and a national builder's merchant where ECSC will provide 24/7/365 cyber monitoring, detection and response support. These wins were equivalent to >20% of the MDR order book. The rail company was a long-standing MDR customer and the builder's merchant was an existing Assurance customer.

Nebula Cloud

There was also the delivery of its first Nebula Cloud service to a new client. Nebula is charged as a monthly subscription and hence does not materially affect the current order book. ECSC announced Nebula in May. It takes ECSC's existing 24/7/365 managed service that uses its proprietary KEPLER artificial intelligence and introduces cloud based service options. This has increased ECSC's addressable market as it offers a lower cost of entry for customers and is designed for the wider reseller base.

KEPLER

KEPLER sits at the core of ECSC's 24/7/365 security monitoring and breach detection services and aids ECSC's engineers at its SOCs in the UK and Australia to process billions of client security events each month in order to identify cyber security breaches at the earliest stage and enable clients to contain and repel attacks before data breaches occur. KEPLER complements the work of ECSC's engineers rather than replacing them. ECSC

maintained investment in its technology base, spending the equivalent to 14% of revenue in FY20.

Partner programme

150 partners

ECSC has successfully built a substantial UK partner channel since 2019 with more than 150 partners at the end of FY20, contributing 4% of revenue (FY19: 2%). 30% of the partners have been active to date with 163 referral leads and 28 partner sales. And the channel accounted for 13% of ECSC's 90 new clients in 2020. Partners range from individual IT consultants that refer opportunities to the ECSC sales team to IT VARs with their own sales teams.

Cyber security represents an attractive growth market but resellers recognise the need for specialist skills and are therefore happy to refer business. From ECSC's perspective the indirect channel extends its sales reach and the margin sacrifice is equivalent to ECSC's own cost of sales. Recruitment will likely slow going forward as ECSC focuses on bringing on only larger partners and developing the existing base.

During FY20, many of these partners were focused on helping clients establish remote and cloud-based working. These working practices present additional cyber security challenges and we anticipate increased indirect sales going forward.

Outlook

Two significant MDR contract wins

FY21 has started well with the company announcing two significant contract wins in its MDR division in February. One is a service extension with a major UK charity that was an existing MDR customer and was originated from ECSC's Partner Programme. The other customer, a national leisure group, is a new client win. The contracts are worth more than £550k over an initial three year period.

Eleven new Assurance clients

ECSC also gained eleven new clients within its Assurance division during January for a wide range of consultancy engagements across multiple sectors. Four of these clients were secured through the Partner Programme.

The MDR contract wins will increase recurring revenue and should help to increase gross margins through higher utilisation of its Security Operations Centres in the UK and Australia. The Assurance contract wins are encouraging given the impact of COVID-19 on consultancy engagements in 2020 and the Assurance division represents the main source of MDR clients.

Market opportunity

Remote working and accelerated cloud adoption has increased the number of attack surfaces

The acceleration in the shift to remote working and accelerated cloud adoption occasioned by the pandemic has increased the number of potential cyberattack surfaces. At the same time, the economic and logistical disruption caused by COVID-19 has resulted in some delays in cyber security spending, described as a 'compliance debt'. There is also some evidence of longer sales cycles in larger managed services contracts and tighter scoping of engagements resulting in lower initial Average Order Values and shorter managed service contracts as organisations remain cautious about the macro outlook.

Two thirds of organisations will increase outsourced cyber resilience work during 2021

According to a survey conducted on behalf of NCC Group (NCC.L) by Opinium Research, two thirds of organisations will increase outsourced cyber resilience work during 2021. This rises to 70% in the private sector and falls to 58% in the public sector. Much of this relates to decisions taken in 2020 in response to the pandemic that accelerated the shift to cloud-based computing and increased remote working. The survey, that covered 290 cyber decision makers and was conducted in January, found:

- understanding the threat landscape post COVID-19 was 2021's biggest challenge

- 30% of respondents reported delays and/or cancellations to cyber resilience projects
- 70% see the increased roll out of cloud infrastructure as a challenge to cyber security
- 39% report increases to insider threats but 52% of this relates to increased remote working
- 20% report furloughing staff responsible for cyber resilience programmes

A report from the UK government in February (Department for Digital, Culture, Media & Sport) estimates that almost 50,000 people are now employed in UK cyber security, an increase of 9% during 2020. The majority (65%) of cyber security employment remains based within larger firms (>250 employees). That said, the number of cyber security firms has increased 21% in 2020 to c. 1,500 and the majority are either small (10-49 staff; 22%) or micro (1-9 staff; 57%).

ECSC sits at the top end of the small category and is able to offer much greater flexibility than larger companies but much greater expertise and a higher level of service, including 24/7 monitoring, than smaller companies.

Increased enforcement of regulation

The number and levels of fines being levied by the Information Commissioner's Office (ICO) is starting to increase following the introduction of new rules under the General Data Protection Regulation (GDPR) that came into effect in May 2018.

Ticketmaster UK

In November, the ICO fined Ticketmaster UK £1.25m for failing to keep its customers' personal data secure. The ICO found that the company failed to put appropriate security measures in place to prevent a cyberattack on a chat-bot installed on its online payment page. The data breach, which included names, payment card numbers, expiry dates and CVV numbers, potentially affected 9.4m of Ticketmaster's customers across Europe including 1.5m in the UK.

Marriott International Inc

In October, the ICO fined Marriott International Inc £18.4m for failing to keep millions of customers' personal data secure. Marriott estimates that 339 million guest records worldwide were affected following a cyberattack in 2014 on Starwood Hotels and Resorts Worldwide Inc. The attack, from an unknown source, remained undetected until September 2018, by which time the company had been acquired by Marriott.

The ICO's investigation found that there were failures by Marriott to put appropriate technical or organisational measures in place to protect the personal data being processed on its systems, as required by the General Data Protection Regulation (GDPR).

British Airways

Also in October, British Airways was fined £20m for failing to protect the personal and financial details of more than 400,000 of its customers. An ICO investigation found the airline was processing a significant amount of personal data without adequate security measures in place. This failure broke data protection law and, subsequently, BA was the subject of a cyberattack in June 2018, which it did not detect until September 2018 and was only alerted by a third party.

ICO investigators found BA ought to have identified weaknesses in its security and resolved them with security measures that were available at the time. Addressing these security issues would have prevented the 2018 cyberattack being carried out in this way, investigators concluded.

The fines, although lower than the theoretical maximums, represent a huge increase on the previous regime

In all three instances, the ICO considered the economic impact of COVID-19 on the businesses before setting a final penalty. The fines, although lower than the theoretical maximums, represent a huge increase on the previous regime and is focusing attention on the need to invest in cyber security. For all but the largest companies, third party service provision is the only realistic option and ECSC has the technology, expertise and processes to capitalise on the opportunity.

Managed Detection & Response

24/7/365 'eyes on glass'

ECSC's Security Operations Centres in the UK and Australia providing true 24/7/365 'eyes on glass' monitoring, alerting and incident response to clients. Australia is a trusted regulatory/government location rather than offering cost-saving through offshoring. The use of SOCs in different time zones also addresses the challenges of recruiting and retaining staff willing to work night shifts.

ECSC's Managed Detection & Response division delivers a wide range of managed technologies that can be categorised as Protect, Detect and Respond.

Protect systems are designed to block attacks without requiring time-consuming analysis and investigation:

- Firewalls to provide external network protection and internal segmentation of critical systems
- Web Application Firewalls (WAFs) deliver enhanced attack blocking for Internet-facing systems
- Intrusion Prevention Systems (IPS) are designed to automatically block suspicious traffic
- Internal and external scanning to confirm an organisation's current vulnerability status

Detect systems form part of the overall Security Information & Event Management (SIEM) solution. These combine cyber security event sources, such as Intrusion Detection Systems (IDS), System Logging and File Integrity Monitoring (FIM). This is supported by ECSC's proprietary KEPLER AI engine to correlate events and support expert engineer analysis and breach identification.

Respond, delivered by ECSC's Incident Response Team, focuses on:

- Investigation – confirm the scope and nature of the breach
- Containment – limit the damage and block further intrusions
- Recovery – restore IT systems and related business functions
- Communications – help with timely communications both internally and externally

Nebula Cloud

Cloud-based service

In May, ECSC announced the Nebula Cloud cyber security breach detection service. This takes the existing 24/7/365 managed service, that uses KEPLER and introduces cloud-based service options. This increases the addressable market as ECSC is able to offer a lower cost point of entry and is designed for the wider reseller base to sell.

Nebula Cloud enables users to collect, store, and use AI to analyse IT system logs and generate 24/7 alerts to potential cyber security breaches. This system, when combined with the ECSC mature Security Operations Centres, expert management, and incident response, gives a fully functioning Security Orchestration, Automation and Response (SOAR) and/or Security Information and Event Management (SIEM) service.

A SIEM collects and aggregates log data from multiple devices (firewalls, network appliances, remote workers, cloud systems etc) and then identifies, categorises and analyses incidents and events. A SIEM examines log data for patterns that could indicate a cyberattack, then correlates event information between devices to identify potentially anomalous activity and issues alerts accordingly.

SOAR platforms combine comprehensive data gathering, case management, standardisation, workflow and analytics to enable organisations to implement sophisticated defence-in-depth capabilities. A SOAR integrates all of the tools, systems and applications within an organisation's security toolset and enables the security team to automate much of the incident response workflows.

The service is being made available in three variants that are set at lower price points than ECSC's traditional MDR offering and there are no long term contract requirements.

Assurance services

Highly qualified

All of ECSC's consultants are highly qualified with a minimum qualification of the Certified Systems Security Professional (CISSP). The company's PCI specialists are all Payment Card Industry Qualified Security Assessors (PCI QSA) and the ISO 27001 specialists have all passed the ISO 27001 Lead Auditor examination. ECSC was also the UK's first PCI cyber security Level 1 Service Provider.

Testing

ECSC offers a wide range of security testing services, including:

- Annual external and/or internal penetration testing
- Specific application penetration testing
- Code auditing
- Social engineering testing

ISO 27001

ECSC can help clients prepare for the UKAS/ANAB accredited certification body assessment. If a client is already certified, or following a successful certification project, ECSC can help clients to manage and maintain their Information Security Management System.

Cyber Essentials

Cyber Essentials is a cyber security standard introduced by the UK government in 2014 that aims to provide organisations of all sizes with basic, cost-effective protection against the most common Internet-based threats.

ECSC is a Certifying Body for the Cyber Essentials programme; this means it can conduct an assessment, report the outcome to the Accreditation Body (IASME), and ultimately, issue certificates.

Cyber Security Review

ECSC's Cyber Security Review is designed to assess the key aspects of an organisation's IT security related infrastructure, processes and technical management capabilities, and

balance these against the cyber threats that are most relevant to a business. As well as identifying potential vulnerabilities, the review will also recommend targeted improvements.

An ECSC Cyber Security review utilises three essential components, all unique to ECSC:

- **ECSC Cyber Security Priorities** - areas of IT security protection that directly impact on an organisation's risks of a serious cyber security breach.
- **ECSC Cyber Security Matrix** - a scoring tool covering an organisation's current capability and the risks that it faces.
- **ECSC Cyber Security Quadrant** - an Executive level reporting system that provides management with a clear picture of an organisation's current position and enables resource decisions.

Payment Card Industry Data Security Standard (PCI DSS)
As Qualified Security Assessors (QSAs), ECSC's role is to:

- Help organisations understand their PCI DSS compliance obligations and options
- Support organisation through a development programmed to deploy compliant systems (and remove others from scope)
- Assess an organisation against the standard, either as a Merchant reporting to its bank, or as a Service Provider.
- ECSC also supports clients through to compliance following a breach of card data.

Exhibit 3: Accreditations
Payment Card Industry (PCI) DSS Level 1 Certified Managed Security Services Provider
A CREST Member Company – a recognised level of expertise in security and penetration testing
Certified to ISO 27001 in 2006 within one month of its release
ISO 9001 certification covering consulting and security management systems
ISO 20000 certification covering managed security services
PCI Qualified Security Assessor (QCA) accreditation

Source: Company

Summary financials

Exhibit 4: Income statement Year End December (£000s)	FY 2018A	FY 2019A	FY 2020A	FY 2021E	FY 2022E
Revenue	**5,382**	**5,905**	**5,663**	**6,563**	**7,898**
YoY Growth	*35%*	*10%*	*-4%*	*16%*	*20%*
Cost of sales	(2,642)	(2,545)	(2,115)	(2,572)	(2,845)
Gross profit	2,740	3,360	3,548	3,991	5,053
Gross margin	*51%*	*57%*	*63%*	*61%*	*64%*
Other income	152	263	297	230	-
Sales & Marketing costs	(1,817)	(1,958)	(1,713)	(1,919)	(2,091)
Administrative expenses	(2,333)	(2,369)	(2,403)	(2,763)	(3,012)
Total operating expenses	**(3,998)**	**(4,064)**	**(3,819)**	**(4,452)**	**(5,103)**
YoY growth	*-23%*	*2%*	*-6%*	*17%*	*15%*
Operating (loss)/Profit before Exceptional Items	(1,027)	(593)	(55)	(361)	50
Exceptional items	(120)	(6)	(65)	-	-
Operating (Loss)/Profit	**(1,258)**	**(704)**	**(271)**	**(461)**	**(50)**
Amortisation	(175)	(377)	(168)	(179)	(179)
Depreciation	(217)	(217)	(312)	(335)	(335)
Adj. EBITDA	**(635)**	**1**	**375**	**153**	**564**
Adj. EBITDA margin	*-12%*	*0%*	*7%*	*2%*	*7%*
Reported EBITDA	(866)	(110)	209	53	464
Net interest	1	(46)	(48)	(50)	(50)
Adj. profit before tax	**(1,026)**	**(639)**	**(153)**	**(411)**	**(0)**
PBT margin	*NEG*	*NEG*	*NEG*	*NEG*	*0.0%*
Profit before tax (reported)	(1,257)	(750)	(319)	(511)	(100)
Tax	19	(26)	50	-	-
Tax rate	*NA*	*NA*	*NA*	*NA*	*NA*
Profit after tax from continuing operations (normalised)	(1,007)	(665)	(103)	(411)	(0)
PAT margin	NEG	NEG	NEG	NEG	0%
Profit after tax from continuing operations (reported)	(1,238)	(776)	(269)	(511)	(100)
PAT margin	NEG	NEG	NEG	NEG	NEG
Loss for the year	(1,238)	(776)	(269)	(511)	(100)
Shares in issue (basic)	9,098	9,098	10,007	10,007	10,007
Shares in issue (diluted)	9,556	9,759	10,913	10,913	10,913
Earnings per share (basic) (p)	(13.6)	(8.5)	(2.7)	(5.1)	(1.0)
Earnings per share (diluted) (p)	(13.0)	(8.0)	(2.5)	(4.7)	(0.9)
Adj. earnings per share (p)	(10.5)	(6.8)	(0.9)	(3.8)	(0.0)
PER	NEG	NEG	NEG	NEG	NEG
EV	6.9	7.2	6.4	6.4	6.3
EV/Sales	1.3	1.2	1.1	1.0	0.8
EV/EBITDA	NEG	>100	17.0	41.9	11.2

Source: Company reports and Allenby Capital estimates

Exhibit 5: Cashflow

Year End December (£000s)	FY 2018A	FY 2019A	FY 2020A	FY 2021E	FY 2022E
Loss before taxation	**(1,257)**	**(750)**	**(319)**	**(511)**	**(100)**
Adjustments for:					
Amortisation	175	177	168	179	179
Depreciation of PPE	217	217	137	335	335
Loss on disposal of equipment	-	(1)	(4)	-	-
Share-based payment charge/(credit)	111	105	101	100	100
Operating profit before movements in working capital	**(754)**	**(6)**	**306**	**144**	**555**
(Increase)/decrease in inventories	35	(8)	17	(1)	-
Decrease / (increase) in trade and other receivables	(148)	(349)	(264)	(178)	(201)
Increase / (decrease) in trade and other payables	111	428	268	215	200
Cash flow from operations before tax	**(756)**	**52**	**377**	**180**	**554**
R&D tax credit received	122	152	343	230	-
Interest received	-	-	-	-	-
Net cash flow from operations	**(634)**	**204**	**720**	**410**	**554**
Acquisition of property, plant and equipment	(105)	(129)	(5)	(50)	(80)
Disposal proceeds	-	16	6	-	-
Development costs capitalised	(187)	(194)	(194)	(195)	(195)
Net cash flow from investing activities	**(292)**	**(307)**	**(193)**	**(245)**	**(275)**
Proceeds from issue of shares	-	-	446	-	-
Net cash flow from financing activities	(21)	(196)	244	(195)	(195)
Effects of exchange rates on cash and cash equivalents	-	-	-	-	-
Net increase / (decrease) in cash and cash equivalents	**(947)**	**(299)**	**771**	**(30)**	**84**
Cash and cash equivalents at beginning of period	**1,597**	**650**	**351**	**1,122**	**1,092**
Cash and cash equivalents at end of period	**650**	**351**	**1,122**	**1,092**	**1,176**

Source: Company reports and Allenby Capital estimates

Disclaimer

Allenby Capital Limited ("Allenby") is incorporated in England no. 6706681; is authorised and regulated by the Financial Conduct Authority ("FCA") (FRN: 489795) and is a member of the London Stock Exchange. This communication is for information only it should not be regarded as an offer or solicitation to buy the securities or other instruments mentioned in it. It is a marketing communication and non-independent research and has not been prepared in accordance with the legal requirements designed to promote the independence of investment research, and is not subject to any prohibition on dealing ahead of the dissemination of investment research. The cost of Allenby research product on independent companies is paid for by research clients.

This communication is for the use of intended recipients only and only for distribution to investment professionals as that term is defined in article 19(5) of The Financial Services and Markets Act 2000 (Financial Promotion) Order 2005. Its contents are not directed at, may not be suitable for and should not be relied upon by anyone who is not an investment professional including retail clients. Any such persons should seek professional advice before investing. For the purposes of this communication Allenby is not acting for you, will not treat you as a client, will not be responsible for providing you with the protections afforded to clients, and is not advising you on the relevant transaction or stock. This communication or any part of it do not form the basis of and should not be relied upon in connection with any contract.

Allenby uses reasonable efforts to obtain information from sources which it believes to be reliable. The communication has been prepared without any substantive analysis undertaken into the companies concerned or their securities, and it has not been independently verified. No representation or warranty, express or implied is made, or responsibility of any kind accepted by Allenby its directors or employees as to the accuracy or completeness of any information in this communication. Opinions expressed are our current opinions as of the date appearing on this material only and are subject to change without notice. There is no regular update series for research issued by Allenby.

No recommendation is being made to you; the securities referred to may not be suitable for you and this communication should not be relied upon in substitution for the exercise of independent judgement. Neither past performance or forecasts are a reliable indication of future performance and investors may realise losses on any investment. Allenby shall not be liable for any direct or indirect damages including lost profits arising from the information contained in this communication.

Allenby and any company or persons connected with it, including its officers, directors and employees may have a position or holding in any investment mentioned in this document or a related investment and may from time to time dispose of any such security or instrument. Allenby may have been a manager in the underwriting or placement of securities in this communication within the last 12 months, have received compensation for investment services from such companies within the last 12 months, or expect to receive or may intend to seek compensation for investment services from such companies within the next 3 months. Accordingly, recipients should not rely on this communication as being impartial and information may be known to Allenby or persons connected with it which is not reflected in this communication. Allenby has a policy in relation to management of conflicts of interest which is available upon request.

This communication is supplied to you solely for your information and may not be reproduced or redistributed to any other person or published in whole or part for any purpose. It is not intended for distribution or use outside the European Economic Area except in circumstances mentioned below in relation to the United States. This communication is not directed to you if Allenby is prohibited or restricted by any legislation or registration in any jurisdiction from making it available to you and persons into whose possession this communication comes should inform themselves and observe any such restrictions.

Allenby may distribute research in reliance on Rule 15a-6(a)(2) of the Securities and Exchange Act 1934 to persons that are major US institutional investors, however, transactions in any securities must be effected through a US registered broker-dealer. Any failure to comply with this restriction may constitute a violation of the relevant country's laws for which Allenby does not accept liability.
By accepting this communication, you agree that you have read the above disclaimer and to be bound by the foregoing limitations and restrictions.

Research Recommendation Disclosure
David Johnson is the author of this research recommendation and is employed by Allenby Capital Limited as an Equity Analyst. Unless otherwise stated, the share prices used in this publication are taken at the close of business for the day prior to the date of publication. Information on research methodologies, definitions of research recommendations, and disclosure in relation to interests or conflicts of interests can be found at www.allenbycapital.com. Allenby Capital acts as Nomad and broker to ECSC Group plc.

Allenby Capital, 5 St Helen's Place London EC3A 6AB, +44 (0)20 3328 5656, www.allenbycapital.com