COMPANY NOTE

FY18 pre-close

22 January 2019

ECSC GROUP PLC (ECSC.L)

Firmly back on track

ECSC Group is the UK's longest running full service cyber security provider (Consultancy, Managed Services and Incident Response). It has long-term relationships with >200 blue-chip customers across multiple vertical sectors and provides investors with exposure to the ongoing growth in the cyber security market. ECSC has invested in its technology (including AI) and service capability and can offer its clients a full suite of cyber and information security services and is one of very few mid-market providers with 24/7/365 Security Operations Centre (SOC) cover. This integrated and comprehensive offering represents a key differentiator. Having grown steadily at c. 20% per annum prior to IPO in 2016, ECSC stumbled in its 2017 expansion programme. Today's in-line trading update demonstrates that this distraction is now firmly behind it with FY18 revenue growth of >30% with profitable trading in October and November. The outlook is positive with cyber security high on the corporate agenda and we expect the company will return to sustained profit in 2019. The current share price fails to reflect its current operations or the growth potential and we set a fair value of 170p/share, equivalent to an FY20 EV/Sales of 1.8x, an EV/EBITDA of 13.5x.

- **Cybersecurity.** The demand for cyber security products and services continues to grow rapidly - a function of both increasing levels of regulation around data security but also the sheer proliferation of attacks. Successful attacks and data breaches garner headlines on an almost daily basis. The penalty regime of GDPR is focusing the minds of company boards and the outcome of the BA breach in September could represent a watershed moment.

- **Trading update.** Today's FY18 pre-close reports >30% organic revenue growth with a good performance across both Consultancy (>25%) and Managed Services (>50%). The growth in Managed Services is particularly encouraging as it offers greater revenue visibility as well as larger contract sizes. Consulting added 95 new clients in FY18 and these represent a good source of Managed Services prospects. Since period end, ECSC has announced a further managed services contract win with a major food producer worth £300k over three years, adding >10% to the order book. Year-end net cash was £650k with some working capital expansion in Q4 reflecting the strong end to the year.

- **Forecasts.** Further revenue growth in Consultancy and Managed Services, coupled with higher margins and the full benefit of the previous cost reduction programme, the company should deliver a sustainable EBITDA in FY19.

EXHIBIT 1: SUMMARY OF

Year End: December (£000)	2017A	2018E	2019E	2020E
REVENUE	4,115	5,434	6,460	7,727
ADJUSTED EBITDA	(2,915)	(677)	239	1,031
ADJUSTED PBT	(3,163)	(1,017)	(161)	651
ADJUSTED EPS (p)	(34.2)	(10.3)	(1.2)	7.4
NET CASH	1,536	650	1,038	1,671
EV/REVENUE (x)	1.4	1.2	1.0	0.7
EV/EBITDA (x)	NEG	NEG	26.2	5.5
PER (x)	NEG	NEG	NEG	10.8

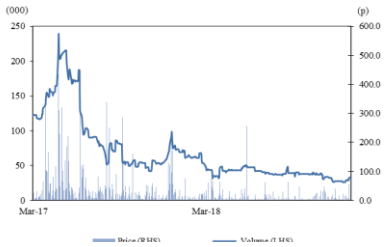
Source: Company; Allenby Capital. **Adjusted PBT, EBITDA and EPS exclude one-off charges and share based charges*

Please refer to the last page of this communication for all required disclosures and risk warnings.

CORPORATE

Current price	**80.0p**
Sector	**TMT**
Code	**ECSC.L**
Listing	**AIM**

Share Performance



	1m	3m	12m
—ECSC.L	18.5%	-13.5%	-55%

Source: Thomson Reuters, Allenby Capital

Share Data		
Market cap. (£m)		**7.3**
Shares in issue (m)		**9.1**
52 weeks	High	Low
	167.5p	**87.5p**
Financial year end		**31 December**

Source: Company Data, Allenby Capital

Key Shareholders	
Ian Mann	**24.8%**
Ravinder Bahra	**11.8%**
Unicorn Asset Management	**15.9%**
Phil Mclear	**5.2%**
Malcolm Hoare	**3.3%**
Artemis Inv. Management	**3.2%**
Lucy Sharp	**2.7%**

Source: Argus Vickers

David Johnson

+44 (0)20 3394 2977

d.johnson@allenbycapital.com

www.allenbycapital.com

EQUITY RESEARCH

INVESTMENT SUMMARY

Proven, premium quality provider of cyber security services

ECSC Group is a proven, premium quality provider of cyber security services with a substantial blue-chip client base where it has developed long term relationships. The breadth and depth of ECSC's in-house developed technologies, methodologies and systems, specifically designed for remote managed services, coupled with two Security Operations Centres (SOCs) that provide 24/7/365 cover represents a comprehensive offering in a fragmented landscape. ECSC delivers its services in the form of Consultancy and Managed Services plus Incident Response complemented by some third-party product sales.

Refocused on its core business

The company has bounced back well after stumbling in its 2017 expansion plan and has returned to >30% organic revenue growth in FY18 – significantly ahead of the market and in line with forecast and trading profitably in October and November. Management refocused on its core strategy of winning Consultancy contracts (95 added in FY18) and converting these into Managed Service customers that provide high levels of revenue visibility. During FY18, Consulting revenue grew >25% and Managed Services >50%. Importantly despite the disruption around the expansion and subsequent restructuring, customer and staff retention levels have remained high and ECSC continues to take market share in growth market.

Consultancy customers represent a good source for Managed Service contracts and ECSC's sales success has continued into FY19 with a further contract win with a major food producer worth £300k over three years for 24/7/365 cyber security monitoring and breach detection. The opening of the Australian SOC substantially increased ECSC's capacity and gross margin is improving as this capacity is being utilised. Today's share price fails to reflect the current operations of the company or the significant growth potential. We set a fair value of 170p/share, equivalent to 1.8x FY20 EV/Sales and an EV/EBITDA of 13.5x.

PROLIFERATION OF ATTACKS AND NEW REGULATION

Strategic issue for company boards

The proliferation of cyber security breaches affecting some of the world's most prominent companies, together with the accompanying media publicity and the raft of new cyber related regulation means that cyber security is a strategic issue for company boards. High profile breaches in 2018 included Marriott, Quora, Ticketmaster, and British Airways and several breaches at Facebook.

GDPR penalty regime

Under the EU's General Data Protection Regulation (GDPR) that came into effect last May, companies have to disclose breaches within 72 hours. GDPR also has a much harsher penalty regime with two levels of fines. The first is up to €10m or 2% of the company's global annual revenue for cyber security breaches. The second is up to €20m or 4% of revenue, whichever is higher, for data security breaches. Other regulation includes New York's Cybersecurity Requirements for Financial Services Companies and Australia's Notifiable Data Breach requirements.

Previously, penalties were insignificant. For example, companies that failed to comply with the UK's Data Protection Act 1998 would be charged a maximum of £500,000 if they leaked data or failed to protect the data they held against potential hacks. There was also little incentive for companies to inform those affected with numerous instances where companies took months before admitting to breaches.

British Airways – test case

September's attack on the web site of British Airways where the personal and financial details of customers making or changing bookings had been compromised is one of the first high profile breaches to occur post GDPR coming into effect and represents

an important test for the new regulatory environment. About 380,000 transactions were affected and the stolen data included name, email address and credit card information (numbers, expiry dates and CVV codes). This data was being sold via the dark web for c. $10 a card at the end of last year. Assuming that BA is found culpable, the level of fine could be up to £250m, if 2% of revenue, and represent a watershed moment and drive further spending in the space.

MARKET GROWTH

The UK market for cyber security services and products was estimated to be worth approximately £3.5 billion in 2017 with a CAGR of 4.5% between 2013 and 2017 (Source: 'Competitive analysis of the UK cyber security sector' published by BIS) and is expected to grow at 10-12% per annum over the next five years. By comparison, ECSC achieved 16.9% CAGR revenue growth in the same period as it continued to take market share.

High-profile data breaches will lead two thirds of companies raising their budgets for cyber security by at least 5% this next year, according to a 2018 EY survey of 1,400 executives. Companies are increasingly allocating money to securing cloud computing and towards analytics software that can monitor their networks and detect unusual activity. Companies are also spending more on training as business activities move into the cloud that are harder to monitor. Careless and unaware employees are still considered the biggest vulnerability.

Managed Security Services growth

The global cyber security market is forecast to grow from $122 billion in 2015 to $202 billion in 2021 (CAGR of 10.6%) (Source: Research and Markets). Within this, Managed Security Services are expected to reach $41 billion by 2022 (CAGR of 16.6%). Demand for Managed Services is being driven by the realisation at many organisations that they do not have the IT departments, specialist resources or complex software necessary to protect their IT systems and increasingly the systems of their customers and suppliers.

Success in converting Consultancy clients

ECSC has demonstrated success in converting its Consultancy clients into Managed Services as its clients recognise that they are ill-equipped to manage the cyber threat. These multi-year contracts increase revenue visibility and are typically much larger than Consultancy contracts. Gross margins are also increasing as the capacity created with the investment in SOC facilities is utilised.

INTELLECTUAL PROPERTY

ECSC has more 18 years' experience in the design, implementation and management of cyber security solutions. ECSC's consultancy-led approach, and its combination of custom methodologies and in-house proprietary technologies, enables the Company to provide individually tailored services to its clients. The Company has significant intellectual property, including bespoke products delivering remotely managed cyber security services and custom-made internal support and delivery systems.

KEPLER Cyber Security Artificial Intelligence

Last June, ECSC launched its KEPLER Cyber Security Artificial Intelligence (AI) product that sits at the core of its 24/7/365 security monitoring and breach detection services and aids the company's engineers 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.

ECSC believes that AI-based products complement the work of its engineers rather than replacing them. Its AI engine takes five billion logs a month for a typical client and generate 200 investigations for the staff at its Security Operation Centre to distil into 10-20 client actions. There are a number of AI-based tools, such as Darktrace, that aim to eliminate the need for engineers but there is a risk that such tools generate too

many false positives for clients to react to and companies lack the specialist skills to understand the outputs.

EXPANSION PROGRAMME AND RESTRUCTURING

Following the company's admission to AIM in December 2016 and associated £5.9m (£5.0m new) fund raising, ECSC undertook a substantial expansion programme that was scheduled to see staff numbers increase from 57 at the time of the IPO to c. 200 by the end of 2018. ECSC also opened a secondary Security Operations Centre in Australia for 24/7 Managed Security Service cover, plus a telesales office in Leeds and a secure facility within the M25.

Delays in the conversion of the pipeline

Although there were initially encouraging signs with a significant increase in the sales pipeline, delays were experienced in the conversion of the pipeline into committed orders. This was partly a function of the lengthening of sales cycles as larger contract decisions require more levels of sign off as the importance of cyber security has increased.

Restructuring completed in November 2017

As a result, the company undertook a restructuring process that was completed in November 2017, resulting in an exceptional cost of £0.3m in FY17 and a further £0.1m in H1 FY18. This included reducing headcount by 27 staff and tighter overhead control. As a result, the operating cost base was reduced by £0.2m per month. Headcount has since increased to 77 members of staff.

Employee and customer retention

In spite of the restructuring, ECSC retained both its core employees and the customer base. The company prides itself on the quality of its working environment and regularly surveys its employees. The feedback is consistently positive. For example, in the latest survey, that took place after the restructuring, 96% of respondents reported that they felt proud of the company and its brand and 91% saw themselves working there in 12 months. Staff retention was 87% in H1 compared with an average of 91% over the last six years.

FINANCIALS

Strong revenue growth

Interims in September demonstrated strong growth with revenue +43% to £2.6m and a substantial reduction in adj. LBITDA to £0.5m (H1 FY17: £1.5m). Consulting revenue increased 36.1% to £1.6m, Managed Services was up 51.5% to £0.8m and Vendor Products by 203% to £0.2m.

The metrics that provide revenue visibility were all encouraging with repeat revenue accounting for 78% of Consulting, the Managed Service order book stood at £2.4m and deferred income was £0.9m. More than 50 new clients were added in Consulting and these represent a good source of Managed Services prospects. Three Managed Services contracts, sourced from Consultancy customers, were signed.

Gross margins increasing; operational gearing

Gross margins in Managed Services have been temporarily depressed by the increased SOC capacity and are now recovering with the addition of new customers. We would anticipate a measured growth in operating costs as additional headcount is recruited.

Today's FY18 pre-close trading update reports organic revenue growth of >30% to c. £5.4m with Consulting revenue increasing >25% and Managed Services >50%. The Consulting division added 95 new clients and this creates a strong sales pipeline for the Managed Services business. The company traded profitably in October and November. Year-end net cash was £650k with a strong end to the year resulting in higher trade debtors (£869k).

The combination of further revenue growth, gross margin appreciation and limited operating cost growth means that we expect ECSC will return to sustained EBITDA profit in 2019.

VALUATION

In terms of the listed peer group, the Assurance division of NCC (NCC.L) represents the closest comparator to ECSC. It offers a number of similar Consultancy services and with the acquisition of Accumuli in 2015, some Managed Services. Adjusted organic growth in the division was 13.8% in FY18. By contrast, ECSC achieved organic growth of >30% in FY18, albeit from a smaller base.

NCC has suffered its own growth problems and in February 2017 initiated a strategic review, completed in June 2017, that concluded that two smaller Assurance divisions, Web Performance and Software Testing, were non-core and Web Performance was sold in March 2018 and Software Testing in May.

Beyond this, Falanx Group (FLX.L, mkt. cap £7.7m), has some similarities albeit at a much earlier stage with acquisitions in the cybersecurity market and the launch of the MidGARD to complement its Assynt intelligence services. Management reported a solid start to FY19 in its AGM statement in September. In November's interims, management reported a 198% increase in Cyber division revenue to £1.4m. This included a first contribution from the assets of First Base, acquired in March 2018, and SecureStorm in July.

Exhibit 2 sets out a broader selection of IT services companies and cybersecurity product companies.

Given the growth in the cybersecurity market and the challenge of securing resource, there has been active M&A activity. Shearwater Group (SWG.L, mkt. cap. £36.8m) acquired Brookcourt Solutions for £30.3m in October. For FY18 (March), Brookcourt generated £20.9m in revenue and £2.0m in EBITDA. This suggests an EV/Sales of 1.4x and EV/EBITDA of 15.2x on the acquisition.

Fair value of 170p/share

ECSC's share price fails to reflect the current operations of the company and the value of its IP or the significant growth potential in both Consultancy and Managed Services. ECSC has consistently taken market share in a growth market and operational gearing should result in accelerating profitability. We set a fair value of 170p/share, equivalent to 1.8x FY20 EV/Sales and an EV/EBITDA of 13.5x.

EXHIBIT 2: SECURITY AND IT SERVICES COMPANIES

			EV/Sales (x)			EV/EBITDA (x)		
Company	Ticker	Mkt. cap (£m)	Historic	FY1	FY2	Historic	FY1	FY2
NCC	NCC.L	514	2.3	2.1	1.9	12.3	11.4	10.1
Falanx Group	FLX.L	11	3.4	1.5	1.0	NEG	51.5	8.9
Blancco Technologies	BLTG.L	61	2.4	2.2	1.9	11.0	11.7	9.4
Corero Network Security	CNSP.L	38	4.7	3.5	2.4	NEG	NEG	NEG
Kainos	KNOS.L	486	4.6	3.2	2.9	29.2	20.1	18.0
Redcentric	RCN.L	109	1.3	1.4	1.4	7.2	7.7	6.9
Nasstar	NASA.L	68	2.8	2.7	2.5	12.0	12.0	10.7
AdEPT Technology	ADT.L	86	2.5	2.2	2.0	11.9	10.4	9.9
Median			**2.6**	**2.2**	**2.0**	**12.0**	**11.7**	**9.9**
Mean			**3.0**	**2.3**	**2.0**	**13.9**	**17.8**	**10.6**
ECSC	**ECSC.L**	**7.3**	**1.4**	**1.2**	**1.0**	**NEG**	**NEG**	**26.1**

Source: Allenby Capital; Refinitiv

BREACHES AND INCREASED REGULATION

Cybercrime equivalent to 0.7% of global GDP

Cybercrime costs the world almost $600 billion annually, according to a report earlier this year by the Center for Strategic and International Studies and McAfee. To put that into context, it represents equivalent to c. 0.7% global GDP, as measured by the IMF.

January's 2018 Global Risks Report from the World Economic Forum ranked both large-scale cyberattacks and major data breaches or fraud among the top five most likely risks in the next decade.

Increased number of records per breach

A study from security consultancy Gemalto concluded that 4.6bn digital records were compromised in the first half of 2018, an increase of 133% despite the number of breaches falling 18.7% to 945. The increase in the number of records per breach reflects the types of breach that occurred in H1. A breach at Facebook allowed hackers to steal public profile information on 2.1bn users and a further 330m users were compromised at Twitter.

In India, an anonymous service allowed users to enter any Aadhaar number, a 12-digit unique identifier assigned to every Indian citizen, and retrieve personal information stored by the Unique Identification Authority on any of India's 1.1bn citizens including their name, address, photo, phone number and email address for 500 rupees (£5). For a further 300 rupees (£3), a user could print an ID card for any Aadhaar number.

Geopolitical threats

The disruptive power of cyberattacks is becoming increasingly clear, particularly in geopolitical threats. For example, a December 2015 cyberattack in Turkey impacted networks used by the country's banks, media and government. Later than month, an attack on Ukraine's power distribution systems cut electricity to 230,000 residents as well as targeting the country's phone system.

Many companies remain unprepared

Companies struggle to comprehend and manage emerging cyber risks and while executives acknowledge the increasing importance of cyber security many companies remain unprepared. According to the PwC 2018 Global State of Information Security Survey (GSISS), 44% of respondents say that they do not have an overall information security strategy; 48% reported that they do not have an employee security awareness training programme and 54% say they do not have an incident-response process.

The hack of Equifax, a major credit reporting company, demonstrated the potential a cyberattack has to ripple through the economy with lenders at risk of consumers freezing their credit and/or the problems of fraudulent loans and credit cards opened in consumers' names with data stolen from Equifax. Between mid-May and July 2017, hackers gained access to systems and potentially compromised the personal information of c. 143m US consumers – c. 55% of Americans aged 18 and over.

BRITISH AIRWAYS

In September, British Airways announced that it had suffered an attack on its web site where the personal and financial details of customers making or changing bookings had been compromised. About 380,000 transactions were affected although the stolen data did not include travel or passport details. The attack occurred between August 21st and September 5th.

The stolen data included name, email address and credit card information – credit card number, expiration date and the three- or four-digit CVV codes. BA does not store the CVV numbers as this is prohibited under the international PCI-DSS standards set out by the PCI Security Standards Council. As such, the card details were intercepted rather than being harvested from a BA database by 'skimming' the payment page before it was submitted. It is believed that Magecart was the perpetrator, the same

group that breached Ticketmaster. In November, it was discovered that the data was available for purchase on the dark web for $10 a card.

As a result of the breach, several banks, including Santander, Barclays and Monzo, cancelled and reissued any credit card that had been used on the BA web site and app during the 15-day vulnerability. This was done on the back of the press reports rather than on BA's advice and before any signs that the data had been misused. The penalty under GDPR could be c. £500m or 4% of revenue but this could be much larger if parent company IAG is held responsible.

GDPR

Under the EU's new General Data Protection Regulations (GDPR) that came into effect in May, companies now have to disclose hacks within 72 hours to the ICO (Information Commissioner's Office). Historically, some companies have waited months and in some cases years before disclosing a breach.

Two levels of fines based on revenue

There are two levels of fines based on the GDPR. The first is up to €10m or 2% of a company's global annual revenue of the previous financial year, whichever is higher, for a cyber security breach. The second is up to €20m or 4% of revenue, whichever is higher, for a data breach. By contrast, under the previous Data Protection Act 1998 the maximum fine from the ICO was £500k.

Lower tier fines will be generally given to organisations who do not integrate data protection "by design and by default" into their services, policies and products and those who do not cooperate with authorities to the satisfaction of a regulator. These fines will also be applied to those who do not assign a data protection officer, or enact these duties, for failing to inform subjects as and when their personal data is compromised, and for not keeping adequate records of data processing.

The higher tier will only apply for the most serious GDPR infringements, including breaching subjects' data and privacy rights, not following the basic principles of data protection, and refusing to comply with demands and requests from the data regulator, such as a refusal to comply with a previous warning or an order on processing data. How an organisation handles user consent will also be considered.

The regulations themselves make clear that all fines issued will be administered on a case-by-case basis, in the spirit of being "effective, proportionate and dissuasive". Separately, individuals will have the right to claim compensation for any damage suffered as a result of the violation.

GDPR also extends to a company's third-party service providers. If an organisation (the controller) uses a data processor, and this processor suffers a breach, then the third party must inform the controller without delay. For example, if a company uses an IT services provider to archive and store customer records and the provider detects an attack and resultant loss of personal data then the IT firm has to promptly notify the controller and the controller has to notify the ICO within 72 hours.

Non-regulatory costs are significant

Although the level of fines will potentially increase substantially, the non-regulatory costs are significant. For example, in 2013, US retailer Target lost millions of credit card numbers and customers' financial details soon appeared for sale online and there was an increase in fraudulent transactions. Target eventually calculated that its net cost after insurance from the breach had been $202m. Of this, regulatory settlements accounted for just $18.5m.

HISTORY

Established in 2000 by CEO Ian Mann and COO Lucy Sharp, ECSC is the UK's longest-running full-service cyber security information provider for Consulting and Managed Services. ECSC initially developed the Firehat Linux-based security operating system in order to secure internal systems. This became the foundation for the range of remotely managed cyber security services. In 2001, ECSC deployed its first client managed services using its own security technologies.

EXHIBIT 3: HISTORY

Year	Event
2000	Company founded by Ian Mann (CO) and Lucy Sharp (COO)
2001	ECSC starts Managed Security Service offering
2003	BS 7799 certification of whole operation
2006	ISO 27001 certification
2007	ISO 9001 certification for consulting and security management systems
2007	Payment Card Industry (PCI) Qualified Security Assessor accreditation
2009	ISO 20000 certification for Managed Security Services
2010	PCI-DSS Level-1 Certified Managed Security Service Provider
2012	Becomes CREST Member Company
2014	Release of first method of blocking the Heartbleed bug to the security community
2015	ECSC SELECT division launched for Vendor products
2016	Admission to AIM
2017	PCI Award for Excellence
2017	Australian Security Operations Centre (SOC) opened
2018	Second PCI Award for Excellence
2018	Launch of KEPLER Artificial Intelligence product

Source: Company

In 2003, the company secured BS 7799 certification covering best practices for Information Security Management as well as how to implement an information security management system. The second part of BS 7799 was later adopted by the ISO as ISO/IEC 27001 in November 2005 and ECSC achieved certification within a month of its release.

In 2010, ECSC became the first UK-based PCI certified provider for a wide range of IT security managed services. ECSC helps clients understand their PCI-DSS compliance obligations and options; support the client through the development programme to deploy compliant systems; and assess the client against the standard either as a Merchant reporting to its bank or as a Service Provider.

Following the 2017 restructuring, Ian Mann resigned as CEO and as a director of the company in April 2018 although he continued to be a full-time employee focused on business development and marketing. Stephen Hammell moved to CEO from Finance Director. Nigel Payne stepped down as non-executive chairman with David Matthewson taking over. Later in April, Ian Mann rejoined the board and Elizabeth Gooch MBE was appointed non-executive director and Steve Hammell and Steve Vaughan, a NED, resigned. Ian Mann was re-appointed CEO in September and Lucy Sharp (interim CEO) resumed her role as COO.

SERVICE OFFERING

Large and diversified customer base

ECSC's service offering comprises Cyber Security reviews; PCI-DSS and ISO27001 compliance assessment and approval; and Penetration Testing. It has a large and diversified customer base in the UK and has security operations centres (SOCs) in the UK and Australia that enables it to offer 24x7x365 cover.

Substantial target market in the UK

ECSC has a substantial target market in the UK of private sector companies that are of a sufficient size that require cyber security protection but not large enough to justify dedicated in-house teams. ECSC also has clients in local government and education but avoids central government as procurement cycles tend to be long and rates low.

CONSULTANCY SERVICES – ECSC ASSURE

Consultancy and testing services from ECSC ASSURE aims to highlight an organisation's information security vulnerabilities and risks and develop appropriate countermeasures, certification and ongoing management. All ECSC consultants are Certified Information Security Systems Professionals and its testers are certified in their testing specialisms. Most consultants are multi-skilled and there is a small number of associates that are also used.

As well as wider technology and process consultancy projects, its range of consultancy services include specific areas such as:

- Cyber Security Review
- ISO 27001 compliance
- PCI DSS compliance
- ICO Security Outcomes for GDPR

Top quartile day rates; optimal utilisation

ECSC can command day rates for its consultants in the top quartile and utilisation rates have been consistently high against the company's own metric of available days of 200 days per annum. It is important to note that ECSC's definition of available days is lower than some consultancies and reflects the need for consultants to retain an amount of downtime for ongoing training and accreditation as well as providing capacity as the division grows. ECSC's management has developed this optimal utilisation rate over many years and partly helps to explain its staff retention rate that is amongst the highest in the sector.

CYBER SECURITY REVIEW

ECSC has been offering cyber security reviews since 2015. The review is designed to assess the key aspects of a company's IT security related infrastructure, processes and technical management capabilities and balance these against relevant cyber threats.

The review comprises:

- Cyber Security Priorities – This cover the areas of IT security protection that directly impact on the risks a company faces of a serious cyber security breach. This is presented in a traffic light action point plan.
- Cyber Security Matrix – ECSC's unique scoring tool that provides an overview of the current level of protection and the risks that an organisation faces.
- Cyber Security Quadrant – An executive-level reporting system that gives an overview of an organisation's security position based on Risk and Capability.
- ICO Security Outcomes – This covers a client's responsibilities under GDPR.

ISO 27001

ISO 27001 is an internationally recognised risk-based standard that sets out a best practice framework for an Information Security Management System (ISMS), helping organisations to protect important information by identifying risks and implementing

relevant controls. The standard has 114 controls but organisations need only to select the appropriate countermeasures based on a risk assessment.

ECSC supports clients in the preparation for, and ongoing management of, certification to the standard and typically involves one or two consultants being on site for around a week. ECSC's engagement involves understanding the impact and probability of risk and then the threat and vulnerability to the risk occurring. It then draws up a risk management strategy that involves reducing risk (improving security countermeasures), accepting some risk, transferring risk (via insurance) and avoiding risk (by changing operating procedures).

Certification demonstrates that a company is serious about security and is increasingly a tender requirement in sectors such as government and finance. Final certification is carried out by an accredited certification body such as BSI.

PCI-DSS

PCI-DSS (Payment Card Industry Data Security Standard) is an information security standard that is mandatory for any organisation that transmits, processes, or stores payment card data (Merchants and Service Providers) for all cards branded by Visa, MasterCard, American Express, Discover and JCB.

First PCI-DSS Level-1 Service Provider

ECSC was the first UK organisation to achieve PCI-DSS Level-1 Service Provider certification for a wide range of IT security managed services. ECSC helps clients understand their PCI-DSS compliance obligations and options; support the client through the development programme to deploy compliant systems; and assess the client against the standard either as a Merchant reporting to its bank or as a Service Provider.

Unlike ISO 27001, the client's consultant is also the final assessor. There are around ten Qualified Security Assessors (QSA) in the UK, that like ECSC, have five or more QSA consultants.

In the case of a breach, a company's losses will come from the repayment of direct fraud losses; payment of the brand's forensic investigation costs; and fines proportionate to the level of compliance discovered. There is also the damage associated with a breach's adverse publicity.

TESTING SERVICES

Human element required

ECSC aims to help its clients to identify security vulnerabilities, assess risk and develop an appropriate action plan to improve protection. Whilst there has been a proliferation of automated security testing tools, ECSC's management believes that there still needs to be a human element in order to appreciate fully how vulnerabilities tie together. In many instances, ECSC will find vulnerabilities so serious that they must be immediately reported to the client as there is a significant risk of an immediate breach. This will often result in ECSC providing additional services.

ECSC's range of security testing services include:

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

Consultancy-type services are normally chargeable on a daily basis. ECSC also sells pre-paid consultancy time to support client projects remotely. These are tracked in 15-minute blocks.

MANAGED SECURITY SERVICES

Managed Security Services (MSS) is the outsourcing of clients' cyber security activities to ECSC's Security Operations Centres (SOC) in the UK and Australia. These services typically make use of ECSC's own products although ECSC does make use of some third-party products and this represents a small revenue stream.

Annual revenue from individual MSS clients vary from low thousands of pounds to more than £200k and vary from one to three years. Typically, MSS clients pay either quarterly or annually in advance. For 18 years, ECSC has designed, implemented and managed IT security solutions. It is a fully accredited PCI-DSS Level 1 certified Service Provider and was the first in the UK to offer such managed IT services. It is also listed with Visa Europe as a Level 1 Merchant Agent and a Level 1 Member Agent.

Gravitate towards MSS

Many organisations are concluding that to comply with the required level of security, the architecture, configuration and ongoing management of hosted systems requires a level of skills and experience that are not available in-house. As a result, management has found that over time Consultancy clients tend to gravitate towards MSS rather than build their own in-house capabilities.

The growth of Managed Services recurring revenue is core to ECSC's expansion strategy. During FY17, the company established a second Security Operation Centre in Brisbane, Australia, and an Incident Response Unit in London as well as further investment in its proprietary software, used in its security devices.

As a result, ECSC is able to offer true 24/7/365 managed services rather than relying on night shifts that tend to drive up staff turnover. This differentiator has been key in new sales wins as well as expanding revenue from existing clients that want to use the Australian facility.

ECSC can add a considerable number of new customers without the need for additional staff and increased utilisation will benefit margins. For example, the contracts announced last June (£900k over three years) required no additional staffing costs.

The set up and installation of managed services is chargeable, followed by a fixed monthly management fee. Additional management charges can apply for additional activities, such as out of hours support or incident response.

FINANCIALS

SUMMARY FINANCIALS

6 months to 30 June	2018	2017
	£m	£m
Revenue	**2.6**	1.9
Gross profit	**1.2**	0.9
Gross margin	***46.1%***	*48.2%*
EBITDA (adjusted*)	**(0.5)**	(1.5)
Profit before tax (adjusted*)	**(0.7)**	(1.7)
EPS (adjusted* & diluted) (p)	**(17.6)**	(7.4)
Cash inflow from operations	(1.7)	(0.5)
Change in cash and cash equivalents	**(1.9)**	(0.6)
Net cash	**3.1**	0.9

Source: Company. **before exceptional items.*

Interim revenue increased 43% to £2.6m with Consulting revenue +36.1% to £1.6m, Managed Services up 51.5% to £0.8m and Vendor Products up 203% to £0.2m. The metrics that provide a degree of revenue visibility were all encouraging with repeat revenue accounting for 78% of Consulting, the Managed Service order book stood at £2.4m and deferred income was £0.9m.

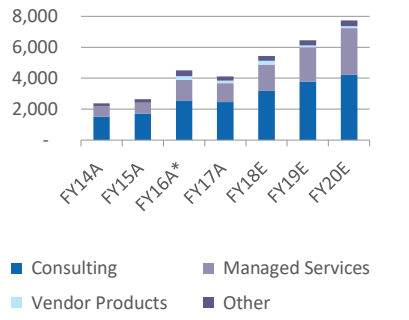
Management is committed to growing the proportion of Managed Services revenue and during H1, the company won three new three-year term contracts that will contribute at least £900k to the long-term order book. Other Managed Services growth came from client renewals, expanded services and upgrades by clients to ECSC's full 24/7/365 service. More than 50 new consulting clients were added in H1 and this represents a good source of Managed Service prospects as Consulting customers often conclude that a Managed Service is a more cost-effective option.

Under the company's previous strategy, management had looked to place greater emphasis on Vendor Product sales as an upsell to Consulting customers and although Vendor Product grew more than 200% it remains small (contributing c. 6% of revenue). As the emphasis has shifted to back to Managed Services sales as well as ECSC's own technology, we expect that Vendor Product sales will reduce in H2 but then likely to stabilise around £0.1m p.a. going forward.

Management reviewed all accounts during H1. This resulted in the company stepping away from some smaller less profitable legacy contracts but this was more than offset by better terms and longer contracts on a number of others. ECSC has limited revenue concentration with the largest customer accounting for less than 10% of group revenue.

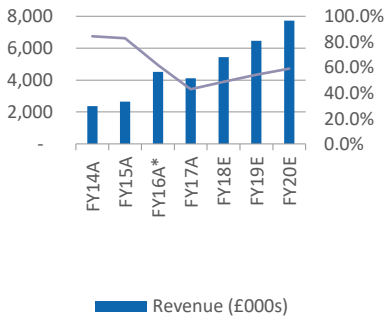
ECSC adopted IFRS15 from 1st January 2018. The adoption impacted the recognition of set-up revenues associated with Managed Services contracts. Historically set-up revenues were recognised on delivery. Under IFRS15. The set-up element also has to be deferred and recognised over the term of the contract. H1 FY17 revenue was reduced by £73k and deferred income was increased by £238k.

Exhibit 4: Revenue breakdown



Source: Company, Allenby Capital * 15 month

Exhibit 5: Revenue and gross margin



Source: Company, Allenby Capital. * 15 months

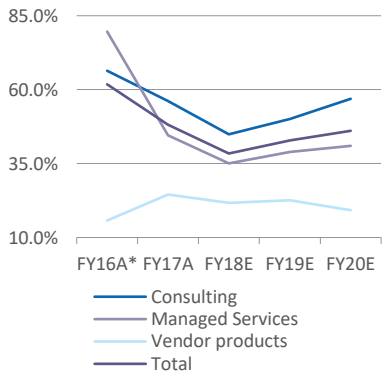
GROSS MARGIN

Gross margin in the Consulting division was slightly stronger at 56.9% (H1 FY17: 56.1%) but improved on H2 FY17 (44.9%). Management reports good utilisation levels and the company continues to secure high day rates. ECSC achieved 75% utilisation against its preferred metric of billable days plus holidays in H1 and expects this to increase to c. 80% by year end and to 82% in FY19 and 85% in FY20.

ECSC's high levels of staff retention and staff satisfaction levels is testament to management's ability to achieve optimal utilisation in a sector that is characterised by severe staff shortages and churn. The co-founders are former consultants and understand that staff require time for ongoing training and certification and there also needs to be some spare capacity as the division continues to grow. As a result, we would anticipate only a gradual further improvement in gross margins and a measured growth in headcount.

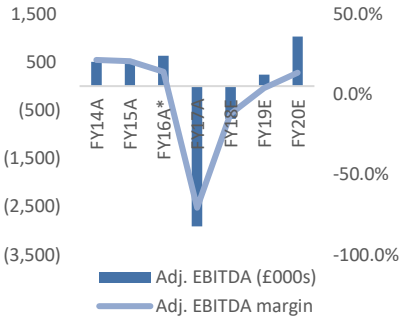
Capacity in Managed Services expanded significantly with the opening of the Australian facility in September 2017 and means that the company can offer a 24/7/365 service. This increased capacity has impacted gross margins (H1 FY18: 41%; H1 FY17: 44.6%) but there was improvement over H2 FY17 35.1%. Managed Services gross margin will continue to expand as utilisation increases. For example, the three contracts secured during H1 required minimal additional costs.

Exhibit 6: Gross margin progression



Source: Company, Allenby Capital. * 15 months

Exhibit 7: EBITDA progression



Source: Company, Allenby Capital. * 15 months

OPERATING COSTS

Sales and marketing costs reduced 30.6% to £0.9m (H1 FY17: £1.3m) and Administrative costs by 6.1% to £1.2m (H1 FY17: £1.3m) following the restructuring that was undertaken in H2 FY17 and there was an additional £99k restructuring charge in H1 (H2 FY17: £275k). H2 will see the full benefits of the cost reduction programme.

The sales team was reorganised in October 2017 with headcount reduced, new leadership installed and the structure adjusted to increase resource focussed on the Managed Services pipeline. Management also reviewed all accounts during H1. This resulted in the company stepping away from some smaller less profitable legacy contracts but this was more than offset by better terms and longer contracts on others.

The company's sales team has six people focused on new business and three on client management and this field sales operation is supported by telephone sales (five) and appointment making (three). New commission structures have been introduced and CEO Ian Mann has direct responsibility for the sales team.

The combination of increased revenue and reduced operating costs resulted in a 64.9% reduction in adj. LBITDA to £0.5m and we expect a further reduction in losses in H2 before returning to profit in FY19.

CASH

Net cash was £0.9m (H1 FY17: £3.1m; FY17: £1.6m). There is some working capital required in the Consulting division but the company has improved collections to <50 days. The Managed Services division has a positive working capital cycle as clients pay upfront on a quarterly or annual basis. Bad debt is very low in the business – less than £50k over the company's history – as struggling companies do not tend to undertake projects that require Consulting services.

Capex returned to more normal levels in H1 (£44k; H1 FY17: £264k) following the investment in Australia in FY17 and the opening of an unmanned facility within the M25. There is some capitalisation of development spend - £80k in H1 (H1 FY17: £75k). Pre-2015, all development spend was expensed as incurred and hence the balance sheet does not fully reflect the investment made in the company's substantial IP portfolio.

FY18 net cash was £650k reflecting some expansion in working capital (debtors of £869k) due to the record levels of trading in Q4.

PROFIT AND LOSS

EXHIBIT 8: PROFIT AND LOSS FORECASTS				
£000s				
Y/E December	FY 2017A	FY 2018E	FY 2019E	FY 2020E
Revenue	**4,115**	**5,434**	**6,460**	**7,727**
YoY Growth	*9.5%**	*32%*	*19%*	*20%*
Cost of sales	(2,353)	(2,790)	(2,961)	(3,167)
Gross profit	1,762	2,644	3,499	4,561
Gross margin	*43%*	*49%*	*54%*	*59%*
Other income	121	140	140	140
Sales & Marketing costs	(2,545)	(1,800)	(1,900)	(2,100)
Administrative expenses	(2,782)	(2,100)	(1,900)	(1,950)
Total operating expenses	(5,206)	(3,760)	(3,660)	(3,910)
YoY growth	*57%*	*(28%)*	*(3%)*	*7%*
Operating (loss)/Profit before Exceptional Items	(3,169)	(1,017)	(161)	651
Exceptional items	(275)	(99)	-	-
Operating (Loss)/Profit	(3,444)	(1,116)	(161)	651
Amortisation	(100)	(150)	(200)	(200)
Depreciation	(154)	(190)	(200)	(180)
Adj. EBITDA	**(2,915)**	**(677)**	**239**	**1,031**
Adj. EBITDA margin	*-71%*	*-12%*	*4%*	*13%*
Reported EBITDA	(3,190)	(776)	239	1,031
Net interest	6	-	-	-
Adj. profit before tax	**(3,163)**	**(1,017)**	**(161)**	**651**
PBT margin	*NEG*	*NEG*	*NEG*	*8.4%*
Profit before tax (reported)	(3,438)	(1,116)	(161)	651
Tax	29	50	50	50
Tax rate	*na*	*na*	*na*	*na*
Profit after tax from continuing operations (normalised)	(3,134)	(967)	(111)	701
PAT margin	*NEG*	*NEG*	*NEG*	*9%*
Profit after tax from continuing operations (reported)	(3,409)	(1,066)	(111)	701
PAT margin	*NEG*	*NEG*	*NEG*	*9%*
Loss for the year	(3,409)	(1,066)	(111)	701
Shares in issue (basic)	9,047	9,098	9,098	9,098
Shares in issue (diluted)	9,176	9,426	9,426	9,426
Earnings per share (basic) (p)	(37.7)	(11.7)	(1.2)	7.7
Earnings per share (diluted) (p)	(37.2)	(11.3)	(1.2)	7.4
Adj. earnings per share (p)	**(34.2)**	**(10.3)**	**(1.2)**	**7.4**
PER (x)	NEG	NEG	NEG	10.8
EV	5.7	6.6	6.2	5.6
EV/Sales (x)	1.4	1.2	1.0	0.7
EV/EBITDA (x)	NEG	NEG	26.1	5.4

Source: ECSC Group plc; Allenby Capital. * pro forma. Adjusted PBT, EBITDA and EPS exclude one-off charges and share based charges

BALANCE SHEET

EXHIBIT 9: BALANCE SHEET FORECASTS				
£000				
Y/E December	FY 2017A	FY 2018E	FY 2019E	FY 2020E
ASSETS				
Non-current assets				
Intangible assets	400	400	367	360
Property, plant and equipment	539	464	329	324
Total non-current assets	**939**	**864**	**696**	**684**
Current Assets				
Inventories	53	30	30	30
Trade and other receivables	1,130	1,029	1,172	1,380
Corporation tax receivable	122	150	100	100
Cash and cash equivalents	1,597	690	1,078	1,711
Total current assets	**2,902**	**1,899**	**2,380**	**3,221**
TOTAL ASSETS	**3,841**	**2,763**	**3,076**	**3,905**
LIABILILTIES				
Current liabilities				
Trade and other payables	(1,618)	(1,588)	(2,060)	(2,180)
Incl.Trade payables	-	(208)	(250)	(250)
Incl. Deferred income	-	(880)	(1,200)	(1,250)
Corporation tax payable	-	-	-	-
Finance leases	(20)	(20)	(20)	(20)
Total current liabilities	(1,638)	(1,608)	(2,080)	(2,200)
Net current liabilities	1,264	291	300	1,021
Non-current liabilities	-	-	-	-
Provisions	-	-	-	-
Deferred tax liability	(15)	10	-	-
Finance leases	(41)	(20)	(20)	(20)
Total non-current liabilities	(56)	10	(20)	(20)
TOTAL LIABILITIES	**(1,694)**	**(1,618)**	**(2,100)**	**(2,220)**
NET ASSETS	**2,147**	**1,145**	**976**	**1,685**
EQUITY				
Share capital	91	91	91	91
Share premium account	5,661	5,661	5,661	5,661
Share option reserve	93	147	147	147
Accumulated losses	(3,698)	(4,754)	(4,923)	(4,214)
Total equity attributable to the equity shareholders	**2,147**	**1,145**	**976**	**1,685**
Net cash/(debt)	**1,536**	**650**	**1,038**	**1,671**

Source: ECSC Group plc; Allenby Capital.

CASH FLOW

EXHIBIT 10: CASH FLOW FORECASTS				
£000s				
Y/E December	FY 2017A	FY 2018E	FY 2019E	FY 2020E
Loss before taxation	**(3,438)**	**(1,116)**	**(161)**	**651**
Adjustments for:				
Exceptional items - IPO costs	-	-	-	-
Grant income adjustment	-	(140)	(140)	(140)
Amortisation	100	150	200	200
Depreciation	154	190	200	180
Loss on disposal of equipment	6	-	-	-
Share-based payment charge/(credit)	93	55	-	-
Operating profit before movements in working capital	**(3,085)**	**(861)**	**99**	**891**
(Increase)/decrease in inventories	(53)	23	-	-
Decrease / (increase) in trade and other receivables	(218)	101	(142)	(208)
Increase / (decrease) in trade and other payables	116	(76)	175	120
Cash flow from operations before tax	**(3,240)**	**(813)**	**122**	**802**
Taxation (paid)/received	178	131	170	50
Interest received	-	-	-	-
Net cash flow from operations	**(3,062)**	**(682)**	**292**	**852**
Cash flows from investing				
Acquisition of property, plant and equipment	(358)	(75)	(60)	(60)
Disposal proceeds	17	-	-	-
Development costs capitalised	(137)	(150)	(160)	(160)
Net cash flow from investing activities	**(478)**	**(225)**	**(220)**	**(220)**
Cash flows from financing activities				
Dividends paid	-	-	-	-
Proceeds from issue of shares	150	-	-	-
Exceptional items - IPO costs	-	-	-	-
Net cash flow from financing activities	**150**	**-**	**-**	**-**
Effects of exchange rates on cash and cash equivalents	-	-	-	-
Net increase / (decrease) in cash and cash equivalents	**(3,390)**	**(907)**	**389**	**632**
Cash and cash equivalents at beginning of period	**4,987**	**1,597**	**979**	**1,078**
Cash and cash equivalents at end of period	**1,597**	**690**	**1,078**	**1,711**
Net cash	**1,536**	**650**	**1,038**	**1,671**

Source: ECSC Group plc; Allenby Capital

PAGE LEFT INTENTIONALLY BLANK

PAGE LEFT INTENTIONALLY BLANK

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, or 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. David Johnson is employed by Allenby Capital Limited as an Equity Analyst.

Tel: +44 (0)20 3394 2977

Email : d.johnson@allenbycapital.com

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.

Allenby Capital acts as Nomad and broker to ECSC Group plc

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