PROGRESSIVE EQUITY RESEARCH

14 August 2018

FALANX GROUP

TECHNOLOGY

FLX.L

5.1p

Market Cap: £13.4m

SHARE PRICE (p)

12m high/low 8.5p/4p

Source: LSE Data

KEY INFORMATION

Enterprise value	£12.4m
Index/market	AIM
Next news	Interims -November
Gearing	N/A
Interest cover	N/A

FALANX GROUP IS A RESEARCH CLIENT OF PROGRESSIVE

ANALYSTS

Maggie Schooley

+44 (0) 20 7781 5312

mschooley@progressive-research.com

Gareth Evans

+44 (0) 20 7781 5301

gevans@progressive-research.com

Falanx Group

Strong market dynamics with consolidation opportunities

Falanx has established itself as a trusted advisor in the cyber security sector through the high-quality execution of its cyber services proposition, based on a methodology and set of processes that have been built up over many years, enabled by strong technology and experienced analysts. The Falanx Group offers an opportunity to invest directly in the growing cyber security market while gaining exposure to the benefits of M&A consolidation in a fragmented segment, led by an experienced team with a proven track record.

- Growth in cyber security spend is forecast to hit $170bn globally by 2020 from an estimated $96bn in 2018. Robust spend, the introduction of more stringent data protection legislation and organisations' growing focus on protecting themselves from increasing cyber threats underscore the growth dynamics to which the Falanx Group is exposed.
- Falanx is one of the few UK listed cyber security firms that can directly offer its clients a comprehensive suite of cyber services driven by an understanding of a client's maturity and ability to successfully absorb and implement a cyber framework. The Group's services are enabled by its proprietary and 3rd party technologies, access to global intelligence and experienced cyber analysts. The Group has established itself as a trusted advisor, allowing it to sell more sophisticated services across its client base and building a recognisable brand in the cyber security market.
- The cyber security landscape is a fragmented one which is ripe for consolidation. Having recognised this, the Falanx Group has implemented a clear and direct strategy of consolidation. Under the leadership of CEO Mike Read, the Group has identified a pipeline of targets which are straightforward to integrate, and which will allow the group to enhance and expand its existing portfolio of clients and services. This will facilitate cross selling of its more advanced managed detection and response services (MDR).
- A brief summary of our near-term forecast may be viewed below with further detail starting on page 20 in the Financial section and a Financial summary on page 31.

FYE MAR (£M)	2016	2017	2018A	2019E	2020E
Revenue	1.8	2.7	3.0	7.1	9.3
Adj EBITDA	(2.3)	(1.2)	(1.6)	0.2	1.0
Fully Adj PBT	(2.6)	(1.7)	(1.7)	0.1	0.9
Fully Adj EPS (p)	(3.8)	(1.5)	(0.6)	0.0	0.3
EV/Sales (x)	6.9	4.5	4.1	1.8	1.3
EV/EBITDA (x)	(5.4)	(10.2)	(7.8)	73.1	12.9
PER (x)	N/A	N/A	N/A	146.9	14.6

Source: Company Information and Progressive Equity Research estimates

TABLE OF CONTENTS

Executive Summary

Introduction to Falanx Group

The Falanx Group is a trusted advisor to clients in assessing, developing and managing their global IT frameworks, policies and procedures against cyber threats. The Group provides professional and consulting services as well as advanced managed detection and response (MDR) services to identify potential attacks and to resolve breaches of security when they occur. Falanx works with government departments within the UK, major corporations, airlines, banks and international non-governmental organisations (NGOs). Falanx has two main business segments: The Cyber Division and the Intelligence Services Division, which are described in detail in this publication.

The cyber landscape is a fragmented one which is conducive to consolidation. Having recognised this dynamic, Falanx is embarking on an acquisition strategy to buy complementary cyber businesses, with a focus on assessment and consulting services. Falanx is looking for businesses that have trusted advisor status across a broad and loyal customer base, which provide cross selling opportunities for Falanx's higher margin MDR services. CEO Mike Read has a long and credible track record in roll-up strategies having created considerable shareholder value through the growth and subsequent sales of both Onemain in the 1990's and Pipex in the 2000's.

Market Backdrop

With the expanding sophistication of the information technology landscape comes considerable and more advanced security threats. The increasing connectivity of the world not only through devices but also through the 'Internet of things' has created greater opportunities for the exploitation of systems and processes. As a result, Governments, companies and individuals are increasingly dedicating financial resources to improving cyber security, policies, procedures and response tactics.

According to Statista, spend in the global cyber security market is expected to reach $170bn by 2020 from $96bn in 2018. Cyber spend remains dwarfed by losses and liabilities associated with cyber-attacks, which Statista estimated at c.$6 trillion globally in 2017. Recognising the divide, governments and regulatory bodies have increased regulation to support sound national cyber frameworks. The recent introduction of regulation such as the EU's global data protection regulation (GDPR), the UK's Data Protection Act 2018 as well as existing regulation in various sectors deemed to be of national critical importance, should underpin increased levels of spend in the market for the foreseeable future. Organisations are increasingly seeking more advanced managed detection and response services (MDR) as threats become ever more sophisticated. There are a limited number of leading-edge cyber security providers able to directly offer MDR services along with complimentary professional security services, of which Falanx is one.

Conclusion

Falanx is one of a scarce few UK listed vehicles that allow investors to invest directly in the fast-growing cyber security market while taking advantage of the consolidation opportunities within the sector. We would encourage investors to meet with the management to gain a greater understanding of the Group's service offering and technology as well its future prospects.

Company Overview

The Falanx Group was admitted to the AIM market in 2013, led by COO and founder John Blamire. Falanx Group assists its clients in assessing and managing global security and cyber threats. The Group works with government departments within the UK, major corporations, airlines, banks and international non-governmental organisations (NGOs) to assist them in;

- Understanding the people they work with and the countries they work in
- Putting into place technical defences to detect and defend against cyber threats
- Adopting a suite of managed services to identify potential threats and weaknesses, resolving breaches of security when they occur.

Falanx has two main business segments: Cyber and Intelligence services. Within Intelligence services, the Group provides geo-political analysis, strategic intelligence and business intelligence analyst services. The division publishes the well-regarded Assynt report which is sold on a subscription basis. It provides consulting services and offers an embedded analyst service to work within a client's organisation. The Cyber Division provides consulting, assessment, awareness and advanced managed detection and response (MDR) services.

The Group is evolving its revenue model from a solely professional services model to one with an increasing level of security as a service (SaaS) revenue. The Intelligence division is a professional services model but with high levels recurring revenues from subscription and embed consultancy while the growing Cyber division, through its monitoring service MidGARD, is increasingly shifting to a recurring model.

Industry Backdrop

Market Size

With the expanding sophistication of the information technology landscape comes considerable and more advanced security threats. Governments, companies and individuals are increasingly focused on the need to improve cyber security policies, procedures and response tactics, which is driving material growth in cyber security spend.

The increasing connectivity of the world not only through devices but not also through the' Internet of things' (IoT) has created greater opportunities for the exploitation of systems and processes. Forbes estimates that in 2017 there were over 1 billion IoT devices in use and estimates that number will rise to 50 billion by 2020. Companies and individuals are often slow to upgrade systems and the pace of software updates is not always compatible with the hardware on which it is run. Aging hardware with unsupported systems often causes problems as security patches are not pushed out to them. Weakness in the patching process is often cited as a major entry point for incidents in post mortem analysis. (theverge.com)

Unlike many other threats and weakness an organisation must prepare for, cyber threat has no physical boundaries. Executive management teams leading organisations often lack the skillset to understand their organisation's level of vulnerability or effectively guide a comprehensive risk strategy to deter cyber threats. In addition, the cost of maintaining a cutting-edge IT infrastructure may be cost prohibitive.

Gartner predicts that global cyber security spending will rise to $96bn (c.£72bn) in 2018, an 8% increase over the previous year, driven by regulatory change, growing awareness of threats and more high-profile breaches. Given the lack of skills inhouse, Gartner predicts outsourcing will be robust with estimated spend on outsourced security services forecast to increase by 11% in 2018 to $18.5bn. According to Statista, spend in the global cyber security market is expected to reach $170bn (£128bn) by 2020.

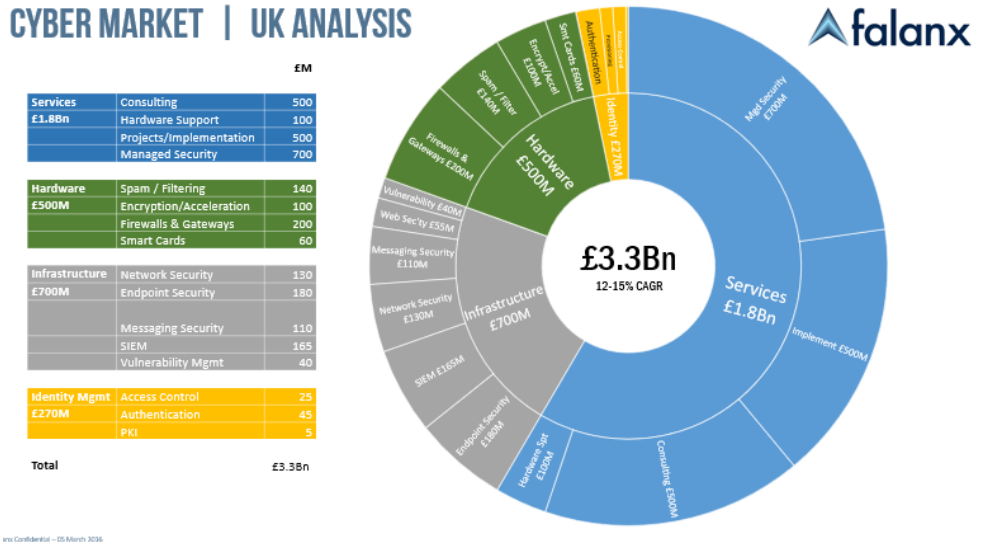
ITgovernance.co.uk estimates that organisations spend only c.5.6% of overall IT budgets on security and risk management. The spend to deter cyber-attack remains dwarfed by the cost of breaches to both organisations and individuals. Statista estimates global hacking losses in 2017 to be c.$6 trillion. A recent survey by RAND estimated the cost of a breach of surveyed individuals at c.$500 per incident but it should be noted that the cost is highly dependent on the type and amount of data stolen. From 2015 data suggest a notable trend to toward targeted attacks on more lucrative targets over small high-volume incidents. In 2015 in the UK, Internet banking fraud rose by 64% to £133.5m with the number of incidents increasing at a lower rate than the prior year suggesting a trend toward focusing on small business and high net worth individuals UK Policy paper on cyber security

The Penemon Institute estimates that the average cost of a data breach for an organisation is c. $4m or an estimated $158 per record. The cost of global data breaches is expected to rise to $2.1trillion by 2019 according to Juniper Research (itgovernanceusa.com). The cost of a breach can vary wildly as can be observed in the Recent High-Profile attacks section starting on page 9 and with further detail in the appendix on page 27.

In 2016, the UK government released a policy paper on cyber security for the period 2016 to 2020. Within the government has ear marked £1.9bn in funding to combat cyber threats to the UK. As part of its policy initiative the government created the National Cyber Security Centre (NCSC) to provide expertise and assistance to UK businesses. The UK government identified state and state-sponsored threats to penetrate UK networks for political, diplomatic, technological, commercial and strategic advantage as presenting increasingly sophisticated threats as technology evolves. Principal areas of focus for such actors are government, defence, finance, energy and telecommunications. Within the report the government clearly outlines its commitment to supporting the cyber security sector in the UK by supporting investment, sponsoring academia and working with that community to ensure customers of and suppliers to the government have robust security processes.

Within the UK spend on cyber has been growing materially over the last several years as organisations better understand the risks and liabilities a cyber breach represents. UK spend on cyber security risen by 47% over the last 7 years from £2.4bn in 2010 to £3.3bn in 2017.

UK Cyber spend



Source: Falanx Group

As can be seen in the exhibit above, UK spend is skewed toward the higher margin services segment which comprises 55% of spend. Within services, managed detection and response (MDR) services, including monitoring, detection alerting and responding, is one of the faster growing areas. Growth in MDR is being driven by more sophisticated threats, scarce resource availability and increasing levels of data being transmitted across networks. This is driving a need for investigative tools and analysts that can react in real time as well as services that have big data capabilities. Gartner predicts that by 2020 15% of midsize and enterprise organisations will be using MDR services from less than 1% currently. Few companies offer comprehensive MDR services currently, but the increasing level of demand is driving managed security service providers (MSSPs) to expand their offerings to include an MDR offering.

Recent Regulatory drivers

As cyber threats evolve and present increasing levels of risk to countries and vital organisation within countries, regulatory bodies have actively passed legislation to create sound frameworks on cyber security. The EU directive on General Data Protection Regulation GDPR was introduced 25 May 2018 and is overseen within the UK by the Information Commissioner's Office (ICO). It supersedes the 1995 EU Data Protection Directive. GDPR in conjunction with the UK's new Data Protection Act 2018 form a major part of the data protection regime in the UK. In the Unites States, the Clarifying Lawful Overseas Use of Data Act of 2108 known as the CLOUD Act was introduced into federal law to modernise data privacy and government surveillance rights and reach for data stored in a cloud computing environment by US companies.

GDPR

The GDPR regulation was, in part, introduced to drive up standards of cyber security across the European Union. There are seven key principles to the legislation, with the 'integrity and confidentiality' principle referred to as the *security principle*. The legislation does not define the measures one has to have in place but requires a level of security 'appropriate' to the risks presented by data processing. The security principle outlines that the holder of data should process personal data securely by means of 'appropriate technical and organisational measures'. (ico.org.uk). The principle calls for holders of information to 'take into account additional requirements about the security of your processing' and 'that appropriate processes are in place to test the effectiveness of your measures and undertake required improvements.' The principle looks at both infrastructure and policies and procedures relating to cyber and physical handling of data.

The legislation encourages the use of encryption and pseudonymisation where appropriate. It promotes certification to enhance transparency and compliance with the regulation and specifically highlights a 'good starting point is to make sure you're in line with the requirements of Cyber Essentials' as a base set of controls (ICO.org.uk). The new legislation put the onus of ensuring robustness of measures on the holder of data in relation to the sophistication of the holder's organisation. The fines for processes and procedures deemed to be inadequate are materially larger than the legislation of the 1998 act. Under the new regulation, the ICO can fine companies up to 4% of global revenue or £20m whichever is greater versus a maximum of £500k in the previous legislation. Companies must inform regulators within 72 hours of discovering a breach. Enhanced investigatory powers have been given to the ICO.

The UK Data Protection Act 2018 covers those areas of processing that do not fall within EU law such as national security and immigration. The act is complementary to GDPR. Both pieces of legislation clearly identify that, with the shift in the market to cloud computing, although the hardware and software may be managed by the cloud provider, security of data remains the responsibility of the client owner and cannot be simply 'outsourced'. The framework cites the need for robust measures to counter data breaches, data loss/destruction and account hijacking. It also highlights the need for secure APIs, authentication processes, access control, and encourages the use of encryption and activity monitoring.

Alongside GDPR, the EU Network and Information Security Directive 2016/1148 came into effect on 10 May 2018. It is a complementary directive to GDPR and is focused on the protection of IT systems in the European critical national infrastructure (CNI). It introduced new breach reporting obligations to a wide segment of industry (banks, transport, energy, etc).

CLOUD ACT

The Clarifying Lawful Overseas Use of Data Act of 2108 introduced in March 2018 amends the Stored Communications act of 1986, and seeks to outline the circumstances under which companies, via warrant or subpoena issued under the Stored Communication Act (SCA), are to provide the government access to stored data regardless the of the geography where it is stored. The Cloud Act states a provider needs to comply with obligations to "…to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States**."** The act has also established bilateral agreements with several nations allowing the US and those nations to make foreign law-enforcement requests request data directly to a US service IT service provider/ technology company rather than through the US government under the mutual legal assistance treaty given the foreign nation has robust standards on human rights and privacy protections. The act formalises the rights of companies to challenge a law enforcement request to protect privacy or civil liberty concerns. In part the CLOUD act was constructed to clarify when complying with foreign laws, like GPDR, would be a breach of US law. Specifically,

article 48 of GDPR prohibits the transfer of data outside the European Union for law enforcement purposes unless specifically agreed under a mutual legal assistance treaty. For those countries that have yet to enter into a bilateral agreement, a request for data may be challenges under “common law.”. The Cloud Act requires that

The recent series of legislation described above has increased organisations’ focus on data protection and storage, but existing regulations such as the FCA’s information technology and data security regulation in UK or the US’s Health Insurance Portability and Accountability Act (HIPPA) (among a myriad of others) have long been drivers of an organisation’s need to have sound cyber policies

Market Accreditations and Influential Standards

In seeking best practice IT standards, many organisations believe it is imperative to align with standards and accreditations that seek to prove to their clients and customers they have the highest levels of protection against cyber threats. Gaining accreditation or certification is one method of instilling trust in an organisation’s processes and procedures. Below is an overview of the standards with which many organisations seek to align. Falanx offer consulting and implementation services as well as ongoing auditing of the accreditations and standards listed below.

ISO 27001 published in 2013 is the International Information Security Management standard. It is part of ISO/IEC27000 series published by the International Organisation for Standardisation and the International Electrotechnical Commission. The standard is known for providing best practice requirements for information security management systems (ISMS), which is an approach to managing sensitive company data to ensure its security. The standard covers people, processes and information technology by using a risk management framework. Those seeking certification must undergo an extensive annual audit process with audit procedures outlines in ISO/IEC 27007.

Cyber Essentials is a set of basis security controls designed by the UK government’s National Cyber security centre (NCSC) launched on 1 October 2016 to support organisations of all sizes to protect against cyber threats. Certification demonstrates a firm’s commitment to protecting firm, customer and supplier’s data. Many organisation (such as the UK government) require such accreditation prior to awarding contracts. Its parent body is GCHQ.

CREST is a professional body that represents the ethical security testing and incident response industry. The CREST accreditation and certifications is built on a framework which measures the capability of cyber security companies and their workforces. The CREST framework has been developed in collaboration with governments and industry players to help identify suppliers whose membership underpins the confidence in the delivery of consistent high-quality technical security services to customers.

IT Health Check (CHECK) is set of vulnerability checks which are measured against high standards the National Cyber Security Centre (NCSC). IT Health check is used for systems that are to be used for HMG and other public-sector bodies processing “Official” or “Secret” information and related critical national Infrastructure (CNI).

Payment Card Industry Data Security Standard (PCI DSS) is not an accreditation to be granted but is a global information security standard administered by the Payment Cards Industry Security Standards Council for cards from the major schemes. It is designed to increase controls around cardholder data in an effort to reduce credit card fraud. Adherence to PCI DSS is a technical requirement for the major schemes data security compliance programs. It is essential for those companies that store, process or transmit card holder data a part of the merchant agreement with the acquiring bank and is audited annually.

Centre for Internet Security (CIS) promote its CIS control standards and CIS benchmarks that identify and highlight best security practices and are recognised as global leading standards for securing IT systems and deterring data attacks. Its employs a method of consensus decision making where by group member agree on the current best practices for a given area of security.

Cloud Control Matrix (CCM) is a standard where compliance is gained by the Cloud Security Alliance (CSA) STAR scheme which promotes the principles of transparency, rigorous auditing and harmonisation of standards. There are three levels of assurance; self-assessment, third party certification and continual audits. CCM is a framework of cloud specific controls aligned with leading standards, best practices and regulation. CCM is one of the leading standards for Cloud security compliance and assurance.

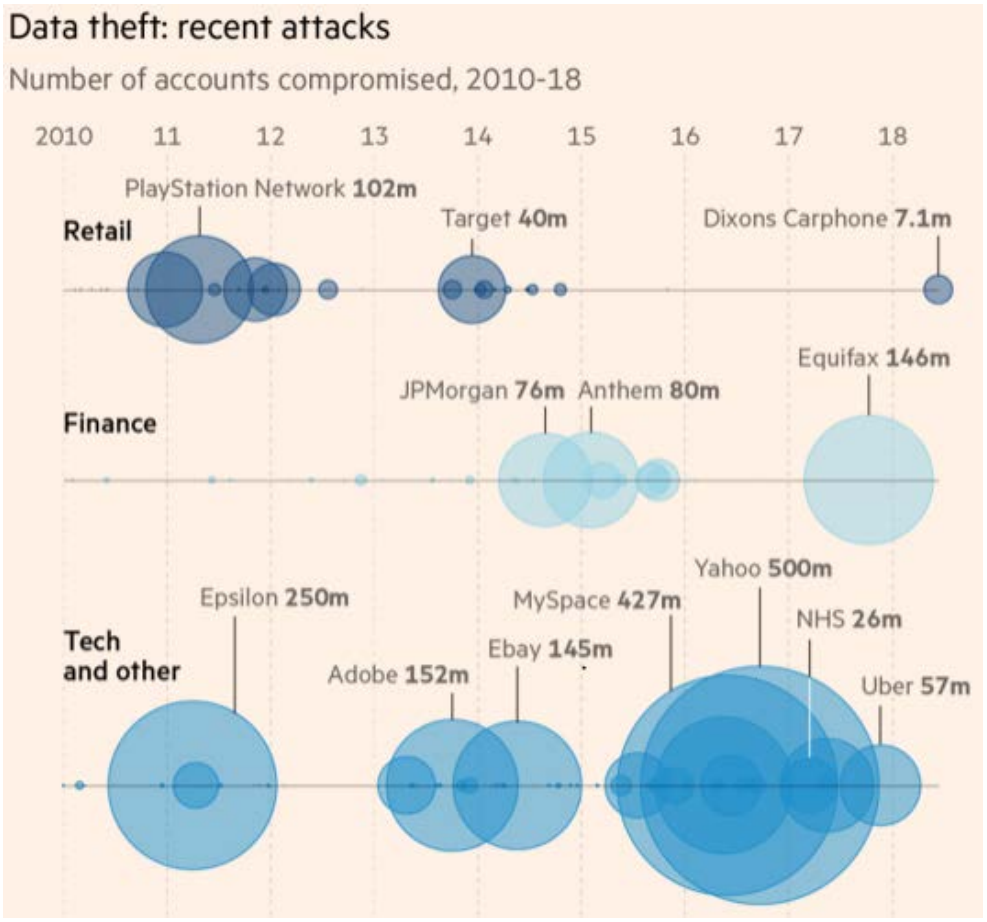
National Institute of Standards and Technology (NIST) is a part of the US department of Commerce which exists to improve industrial standards. NIST's mission is to develop and promote measurements, standards and technology to enhance productivity, facilitate trade and an improve the quality of life." (safety.grainger.com) NIST certifications mainly centre around measurement and calibration testing encompassing a range of technologies that include computer science, mathematics, statistics, and systems engineering. NIST has a cybersecurity programs which promotes the development and use security technologies and methodologies to improve an organisation's ability to address current and future computer and information security challenges.

Recent High-Profile Attacks

In the Appendix on page 27, we have outlined several high-profile attacks for the reader to gain an understanding of the scale of disruption and cost of a major incident. They include the huge problems experienced by Equifax, Maersk and the National Health Service (NHS) among others. In addition, the overview underscores how often capable management teams find themselves bereft of knowledge and questioning how to respond when such an instance occurs. Not only do many organisations with capable management teams lack the necessary knowledge to make informed decisions in a time of attack, internal skillsets to deal with such incidents often do not exist. MDR services which detect and respond to attacks are often secured prior to any incident as part of an organisation's overall security framework. It is highly unlikely a firm will contact a security firm which they do not have a close trusted advisor relationship with during an event. An organisation's inability to act swiftly can cause high degrees of financial and reputational damage over an extended period.

The exhibit below highlights a select group of attacks from 2010 to 2018 where c.2bn records were accessed by hackers. By way of illustration, simply using the suggested figure of $158 per record as cited above, the attacks below would have cost the organisations collectively c. $316m. The exhibit is by no means exhaustive but underscores the point that data breaches are costly.

Data Theft



Source: Financial Times (13.6.18)

Falanx Group

The Falanx Group proposition is based on a methodology and set of processes that have been built up over many years which are enabled by technology and experienced analysts. The Group is segmented into two main service segments; Cyber and Intelligence services.

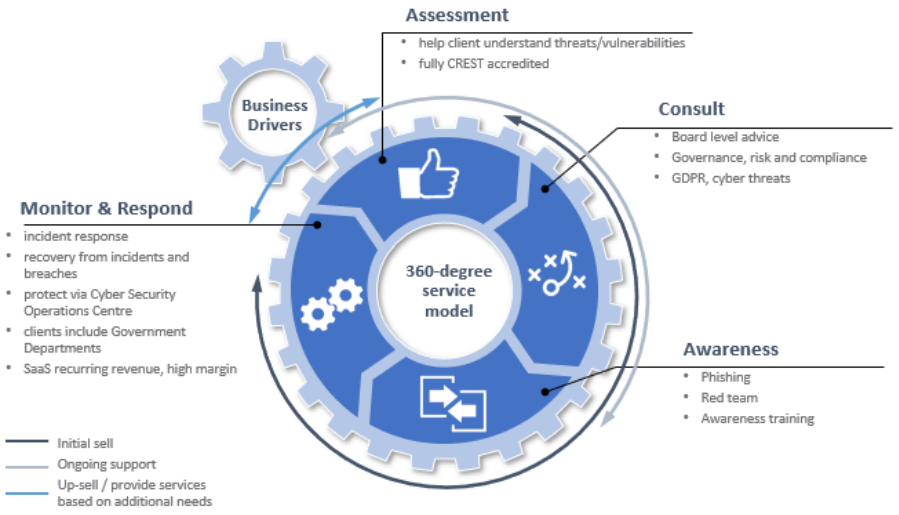
Cyber

Falanx Cyber Services assess the end to end cyber threats within a client's organisation. The Group provides services to its clients to design and implement solutions to identified vulnerabilities, implement best practice standards and gain accreditations. The Group also offers managed detection and response services which augment and support managed professional services.

Falanx's technology framework has been built utilising a bottom up approach. It has created its own proprietary software that it uses in conjunction with select third party applications, to deliver a best in class technology suite with big data capabilities.

Within the Cyber division the Group offers consulting, assessment, awareness, and detection and response services. As depicted in the diagram below the Group offers a 360º service model with services that can be sold into a client various times for a variety of reasons.

Service Offering

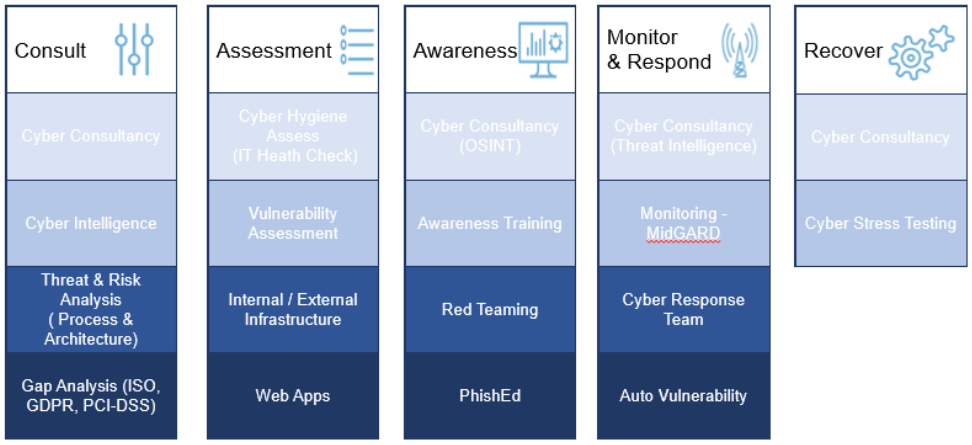


Source: Falanx Group, Progressive Research

When assessing the needs of a client, Falanx takes a holistic view of an organisation to establish its level of maturity, thereby understanding its client's ability to consume cyber services effectively. For example, a client may approach Falanx and request monitoring, also known as managed detection which may have been mandated upon them by a compliance and security framework. For example, all government organisations are mandated to have their networks perpetually monitored. When taking that client on-board Falanx may discover during the on-boarding process, that the exercise may be a futile one as the client lacks the necessary systems or processes to ensure a successful and continuously positive outcome. A simple analogy would be the comparative futility of fitting a burglar alarm to a house whose doors and windows are broken. In this scenario, Falanx will then consult with the client to construct a solution to the vulnerabilities in its systems and processes which will then enable it to effectively consume the mandated service and generate relevant outcome.

The exhibit below, formed on the capability maturity model, broadly identifies the ability of an organisation to consume services based on its behaviours, practices and processes which can reliably and sustainably result in intended outcomes. Reviewing from left to right, the more mature an organisation is, the greater its capacity to effectively consume increasingly advanced cyber services.

Maturity Resilience Services



Source: Falanx Group

The exhibit is useful in broadly understanding why and when an organisation would seek to consume the services Falanx offers. Companies which are immature tend to have ad hoc process and are not efficiently organised and therefore would only be capable of effectively consuming initial level services as outlined on pillar 1, which focuses on preparing and identifying therefore creating a baseline for a cyber defence framework. As an organisation matures its processes follow a regular pattern and it would look to consume services in the second pillar known as repeatable services. Organisations that have defined and well documented processes would then seek to further protect themselves by consuming awareness services, such as training and phishing. The more advanced detection and response services, outlined in Pillar 4, are directed toward companies with processes that are managed and measured. And finally, optimised services shown in pillar 5 would be sought by companies that follow good practices and are able to automate various processes.

Utilising this framework underpins positive outcomes for the more basic services Falanx is contracted to implement. By taking such a service approach, the Group has been able to build strong relationships and grow its reputation as trusted advisor. Establishing a trusted position and understanding which services its clients can consume at various points in their lifecycle, has allowed the Group to expand its more sophisticated MDR services across its client base.

The sales cycle for the services Falanx offers can be a protracted one when dealing with clients that have yet to attain the maturity needed to consume the entry level of services. When dealing with more mature clients, where the Group has built a trusted advisor relationship, the more advanced MDR services are more easily sold. Selling MDR services into organisations where Falanx does not have an established relationship can be an even more protracted effort than selling basic services into less mature organisations. This dynamic is more fully explored in the Roll Up Strategy section on page 17.

Consulting

Every client that Falanx works with consumes its consulting service to some degree. Falanx works with its clients to address the risks that have been identified, to shore up an organisation's security standards or comply with regulations and the highest cyber security standards. The Group's consulting services can range from entry level advice to advising the senior management of the threats to which it is actively exposed to establish effective risk management policies. In addition, the Group provides virtual Chief Information Security (vCISO) consultancy for small to large firms.

Within the consulting division, the Group provides secure architecture services where it works with organisations to review a client's existing IT architecture and/or design an updated secure framework. As well, project assurance services are offered to challenge material projects and provide security oversight and governance. Falanx works with its clients on policy development, offering services which assist clients in developing and implementing policy and control frameworks to enhance protection and provide basic governance

The Group provides audits services and consulting on how to comply with and implement industry standards such as PCI DSS, ISO27001 and Cyber Essentials as well as others which are highlighted in the Market Accreditation and Influential Standards section on page 8. The Group provides guidance on ICO/GDPR regulations, to ensure an organisation is complying with the standards in a manner befitting its size and complexity (see page 6 for further detail on recent regulatory drivers).

Assessment

The Group's assessment services assist its clients in identifying, understanding and preparing for threats and vulnerabilities within their organisations. The Group's services examine a client's cyber resistance and hygiene, charting an organisation's internal and external threat landscape in order to highlight systems, applications and processes that present a risk to cyber-attack

The Group performs vulnerability assessments which are (qualitative tests of an organisation's security controls or known weaknesses within systems on a regular basis to ensure protection and tangibly exhibit the level of defence within an organisation. Its assessments include general security and compliance penetration testing across a client's infrastructure, applications, web applications and platforms. The Group offers mobile assessments which assess threats to mobile devices and applications.

The Group provides IT Health Checks, gap assessments for various regulations and industry standard as well as benchmarking services to validate an organisation's strategy. A more detailed description of the assessment services the Group offers can be found in the appendix on page 26.

Awareness

The Group offers awareness services where Falanx uses open source intelligence techniques (OSINT) to profile a client company and its employees. Falanx uses readily available information such as social networks, forums, business websites, blogs, videos, and news sources. This information is often used within its social engineering services to highlight the human exposure within an organisation. It services include phishing and vishing where target campaigns are created to assist an organisation in understanding the risks associated with one of the most common forms of attack.

The Group' s "red team" services are bespoke and targeted exercises designed to identify organisational weaknesses by adopting an adversarial position. The service simulates a real attack, allowing the Group to deliver pragmatic and effective threat assessments under controlled circumstances. Through its approach, Falanx helps its clients to improve security awareness and adopt a threat led security strategy. Red team services can be both physical and cyber. Information provided by the Strategic Intelligence division can be assimilated into the exercises where appropriate.

Falanx works with clients to train staff of every level, to raise awareness of threats and educate on how respond to those threats therefore increasing the strength of an organisation's barrier to attack. The social engineering services Falanx offers to its clients provides one of the highest levels of value. Organisations that can instil high levels of threat awareness via social engineering services materially decrease risk, as this vector is one of the most exploited by attackers. This service extends to physical aspects of clean desk policies, password protection, security badge protection, among other physical awareness techniques.

Monitor and Respond

Monitoring

MidGARD is the Group's managed detection and response (MDR) service which was launched in February 2017 targeting small and medium enterprises. MidGARD encompasses proprietary IT and third-party software to identify potential attacks. The Group combines best in class technology with skilled cyber security analysts that monitor, report and investigate such threats 24/7/365. MidGARD SOC (security operations centre), is located in the UK and is staffed by SC (security check) and DV (developed vetting) cleared staff.

MidGARD is a service platform utilising open sources technology, big data analytics and machine learning. The Falanx Cyber MidGARD Monitoring Service is comprised of two separate elements, software 'agents' which are installed typically on a client's key servers and/or workstations, allowing communication between the given device and a virtualised collector device. Log collection agents are responsible for the collection of, packaging, encryption and transfer of selected security log data to the Falanx security operations centre (SOC) in real time. The application has a highly flexible log collection capability which also allows collection from networks, endpoints, cloud services and mobile devices when required. A copy of all traffic data is stored for later forensic analysis when necessary.

The client's log data is analysed against a compiled library of known events based on the UK Government's best practice documentation (GPG-13). In addition, Falanx's approach to detection can be distinguished from its peers, as it has taken a multi tenanted approach to its security operations centre (SOC). Such a community-based approach allows the Group to build a broad and rich baseline, based on a library of shared events across a wide range of clients. Threats that emerge in in one sector often move onto another, allowing the Group to quickly identify abnormal activity supported by its previous learnings. By utilising this approach, Falanx can generate a threat pipeline giving context to the observations providing the Group's expert analysts with additional indicators of potentially malicious or undesirable behaviour, thereby enriching the investigation and remediation.

MidGARD categorises alerts as "standard" or "enhanced". "Enhanced" alerts are reviewed by expert analysts and require attention from the customer. Clients are provided daily and monthly alert reports which are highly customisable the implementation of advanced monitoring services such as MidGARD supports advanced compliance procedure for organisations seeking compliance with GDPR and PCI DSS or accreditation such as ISO 27001, among others.

Responding

Clients can enter into a proactive Incident Response contract. This is a managed service that acts like an insurance policy in the event an attack occurs. Ad-hoc response services are offered for companies that find they do not do not have the skills within the company to fully understand an attack and remediate the issues.

Falanx offers, for example post a malware attack, analysis services that support an organisation in understanding the full impact of an incident.

The Group also offers Crisis Management services to support an organisation in all aspects of managing a crisis. This service is not just related to technology but spans across an organisation.

AUTO VULNERABILTY

Falanx offers, automated vulnerability testing services are designed to automatically and regularly test for known vulnerabilities within a client's infrastructure. Automated testing represents a cost-efficient manner of running repetitive tests and is often employed when access to further human resources is limited.

Intelligence Services

The Falanx Intelligence services division provides predictive geopolitical intelligence, research and consulting services to its clients. The division has three segments; The Assynt Report, Embedded Analysts and Intelligence Consulting.

The Assynt report is Intelligence Services', flagship product. The Assynt report is a fortnightly subscription-based product, which provides expert analysis and forward-looking intelligence on strategic issues facing global organisations with interests in emerging markets. Many cyber service providers provide intelligence, often at a high level across wide number of geographies with general intelligence that does not lend itself to making strategic organisational decisions. Falanx Assynt differentiates itself from competitors through its ability to provide predictive and accurate intelligence for regions in which they specialise. Unlike many, Assynt provides firm opinions, forward-looking and actionable analysis of geopolitical and security risks.

The Assynt report is compiled using a global network of well-connected people, providing geo-political insights and commentary of 40 countries on 4 continents. The report covers many African nations, Latin America, the Middle East and Russia. The Group's has a specialisation in Jihadism and its publication 'The Black Banners Monthly' is a well-regarded source of information. The division's large multinational clients use the Assynt report to help them understand, predict, and manage complex risks and issues.

The Intelligence Consulting segment provides strategic intelligence services which assess opportunities and mitigate risks. Its services outline risks and threats in local markets which cover geopolitical systems, fiscal policies, local law and organisational governance policies. The segment's services include pre-market entry intelligence, advice on commercial disputes, corruption, unethical behaviour, political intervention, litigation and situations of force majeure. Business Intelligence services are also offered providing enhanced due diligence reports on suppliers, partners and M&A targets.

For organisations that have greater intelligence needs, the Group offers an Embedded Analyst service. This service provides analyst capabilities on a time share basis for organisations that desire to outsource intelligence for a variety of reasons, be it cost, a dearth of available qualified skills or for ease given Falanx's trusted position. An embedded analyst will have full access to the wider Falanx assets and skill set making the value proposition of an embedded analyst an attractive one to clients.

Routes to Market

The route to market for Strategic Intelligence products and services is mainly though networking at Industry events and by clients who seek out the Group given its reputation. Engagements for embedded analyst services and strategic consulting typically arise from subscribers of the Assynt report taking additional services.

The Cyber division has several route to market strategies. One mechanism involves simply the servicing of inbound inquiries. The Group has a sales team that is wholly dedicated to servicing inbound inquiries, which are high in number. Inbound inquiries are based on the Group's well-known reputation in the market. The team produces 80-100 proposals per month and is currently running at a c. 45% conversion rate. The team typically handles one off engagements in the £3-5k revenue range for many of the repeatable services such as assessment and penetration testing services offered by the Group.

For the MidGARD monitoring service, the Group has employed an indirect sales approach working with seven channel partners. The partners are predominantly IT services providers such CDW (UK), Nasstar, and Sentronex, that enhance and differentiate their own offering by acting as a VAR for MidGARD. Falanx directly employs three members of staff to manage its channel partner relationships. The Group employs a framework agreement with each of its channel partners which is periodically renegotiated. With its increasing level of brand recognition, direct inquiries for its monitoring services are rapidly growing. Response services are sold either as an additional service via the channel partner or can be negotiated directly in many instances.

Revenue Model

Within the Strategic Intelligence division, the revenue model for the Assynt report is a subscription- based one which has strong margin and visibility characteristics. Embedded Analyst services are also charged a function of a full-time employee rate with burden. Contracts are typically up to 1 year in duration and include advance payments. The Intelligence consulting product is charged on a per assignment basis and can have wide-ranging values

Within Cyber the Group is evolving its revenue model from a solely professional services one, to a managed services provider. As can be seen in the exhibit below the Group has several revenue streams. The consulting services are typically bespoke project revenue that tend to deliver margins of 40% or greater depending on the engagement.

The Cyber division assessments are typically repeat revenue (and consequently levels of churn are low and indeed, account revenue can grow with customer expansion), as the gap analysis the Group performs for its clients must be updated to reflect the quick changing threats in the environment. Therefore, the segment generates repeat revenue with an approximate 50% gross profit margin.

The Cyber Division monitoring product's revenue model is a managed service model with software as a service characteristics (SaaS), which should result in increasing revenue visibility as the customer base increases generating higher levels of recurring revenue on average clients are charged a monthly fee of c. £6k but this will vary as function of their size, data collection requirements and duration of contract. Incremental gross margins are up to 70% depending on the level of external services & technologies used in a customer solution.

The response services are charged like an insurance policy. If an incident occurs that incurs a greater charge than the level to which the client is "covered", it will be billed in excess. Therefore, there is an element for both repeat and unexpected revenue with a blended margin of c. 50%.

Cyber Revenue Model

Source: Falanx Group

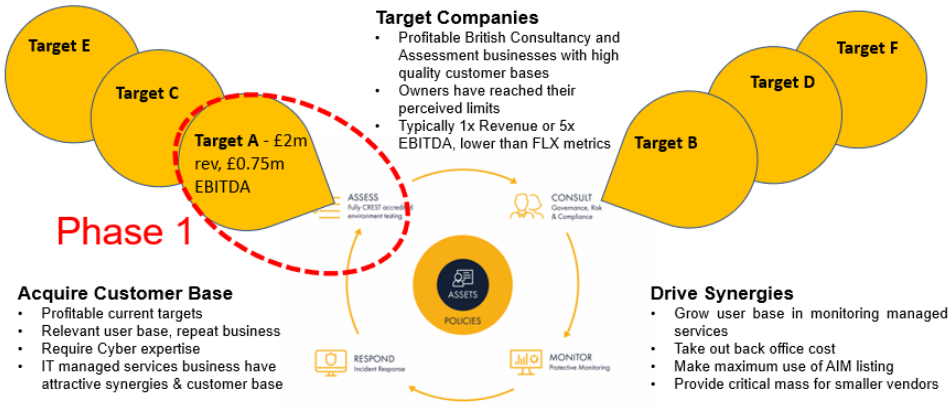
The main operating costs across the group are technology cost license fees, people and data storage costs.

Roll Up Strategy

The Falanx management have identified the cyber security market as a fragmented market with strong growth characteristics, which appears ripe for consolidation under the guidance of an experienced management team.

As can be seen in the exhibit below, the Group's acquisition strategy is to buy complementary cyber businesses, with a focus on assessment and consulting services. Falanx is looking for businesses that have trusted advisor status across a broad and loyal customer base, which predominately purchase services across the initial, repeatable and defined pillars. The Group has compiled a pipeline of targets, which provide cross selling opportunities for Falanx's higher margin MDR products and services. The Group is seeking acquisitions of companies that typically have c.100-200 customers, are straightforward to integrate, are profitable, have the potential to be high cash generative organisations after simple integration, with stable repeat business. Falanx would expect to take out c.5-15% of the targets fixed cost base due to the rationalisation of duplicated costs such as back office, etc. The Group expects to gain cross selling benefits of c. 5 % of revenue in year 1 and 10% by year 2. The Group is targeting businesses at multiples less than its own to take advantage of its listed equity position. In addition, it will employ EMI options to incentivise and retain acquired key staff which we believe is a key differentiator from private equity and other buyers.

Roll up Strategy



Source: Falanx Group

The Group performs in-depth due diligence with a focus on customer retention and utilisation. Considerable focus is paid to understanding the capabilities of tier two management teams and their influence on a customer base. The Group takes care to ensure there are no outstanding unusual warranties or indemnities, non-compete clauses or tax liabilities that could prohibit the realisation of value. Falanx is able to rationalise the acquired cost base as well as drive revenue synergies which given the scalable nature of its platform allows the enlarged Group to capture the benefit of its operational gearing.

To finance its transactions Falanx typically uses a mix of cash, equity, warrants and potentially loan notes. The group will increasingly utilise bank finance for future acquisitions as it expands to reduce share issues. Earnouts and deferred consideration will be used to de-risk transactions as appropriate, with the stipulation that they don't impact the ability to effectively integrate of the target.

Acquisitions

In May 2016 the Group acquired Advanced Security Consulting (ASC) for £0.435m. The acquisition was financed via a mix of cash (£150k) and equity (£285k) as part of a larger company raise. The acquisition of ASC brought consulting, managed services, penetration testing and training services.

In July 2017 the Group acquired Cloudified Ltd for £180,000 of which £80,000 was equity financed. Cloudified is a software defined wide area network (WAN_ vendor. Cloudified brought connective technology, data management and a monitoring platform that complemented the core Falanx cyber technology. Danny Waite the Cloudified Ltd's managing director was appointed Head of Software Development for Falanx Cyber technology.

September 2017 acquisition of AuditSec Service ltd. AuditSec brought cyber security consultancy services to brands across Europe. Richard Morrell AuditSec's Chief Technology Officer joined Falanx in the same capacity.

The Group acquired First Base Technologies in March 2018. The Group raised gross £4.6m at the time of the acquisition (102,222,222 new shares at 4.5p~ represents 64.9% of outstanding capital). Proceeds of the raise were mainly used to fund the acquisition of First Base but also earmarked for working capital, integration, development expenditure and transaction fees. First Base (revenues c£1.8m, £0.6m EBTIDA) was a profitable cyber security testing and consultancy business with a broad customer base of c. 200 customers.

Most recently, the Group announced the acquisition of SecureStorm in July 2018 for an EV of £0.25m, of which £0.1mn was satisfied with the issue of 2.2m shares and the remainder being the assumption of £130k of HMRC debt and a grant of 2m EMI option to Managing Director Tony Richards. SecureStorm had revenues of circa £0.55m for the 12m to June 2018 and was approximately break-even at that point. Synergies have been identified around revenue enhancement (cross selling and utilisation) as well as usual cost sharing. SecureStorm provides cyber security consultancy services and associated regulatory requirements such as GDPR. SecureStorm contributed a Fortune 100 company customer base as well as several UK government departments with which it holds large managed service contracts to the Group. In addition, the acquisition brings Crown Commercial Supplier status, a portfolio of compliance and security process proprietary intellectual property, an exclusive partnership and licence of Edgescan's network scanning technology for use in UK Government, trusted vendor status on the AWS Marketplace. The acquisition will give the combined Group the opportunity to cross sell services such as MidGARD and increased capacity to grow its GDPR consultancy practice

Competitors

Many firms' operating in the cyber space appear to offer similar services, of assessment and penetration testing, accreditation consultancy and audits. Services such as monitoring, detection and responding (MDR) are less widely offered and many firms act as value added resellers (VAR) of those services. Unlike many of its competitors Falanx does not act as a value-added reseller, directly offering a complete set of cyber security services to organisations with varying levels of maturity. Its processes and methodologies, as well as its multi-tenanted approach as described above allow Falanx to differentiate itself from its competitors.

Competitors

Company	Description	Investment	Professional Services	Monitoring	Response	Proprietary Tech IP	Social Engineering	Training	Red Team	Government Consulting	Auto Audit
ECSC	Managed sercurity service provider	Direct through PLC	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No
NCC Group	Provider of software escrow, cyber security and web performance services	Direct through PLC	Yes	Yes	Yes	No	No	Yes	No	No	Yes
Falanx Group	Cyber Security and Intelligence services provider	Direct through PLC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
GRC International	Founded in 2002 as Information Security book publisher	Directly in PLC	Yes	No	No	No	No	Yes	No	Yes	NO
BAE Applied Intelligence	Division of BAE systems	Indirect through BAE systems	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes
BT Security	Division of British Telecom	Indirect through BT	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes

Source: Falanx Group, Progressive Research –

The chart above maps Falanx direct services against those of its UK listed competitors. Falanx clearly stand above most of its competitors in being able to offer a wide suite of direct services

Both NCC Group and BAE Applied Intelligence provide a more compatible offering but are part of larger groups with broad activities which does not allow UK investors to directly invest in the cyber security assets alone. In addition, as we have previously noted, Falanx also offer investors the ability to participate in consolidation of the cyber security market led by an experienced team.

Appendix on page 28 contains an overview of the Group's global competitors. The overview highlights the wide-ranging competing offerings in the cyber space across both listed and private of various sizes. Although several of the listed organisations are very large, the overview provides investors understandable benchmark as Falanx expands its offering.

Financials

Financial Highlights

FY2018A saw 10% revenue growth, delivering £3.0m of revenue versus £2.7m in FY2017A. The Intelligence delivered 5% y/y growth while Cyber delivered 18.5% y/y revenue growth. It should be noted the FY2018A financials include only one week of contribution from the First Base acquisition and its benefit may be viewed in the Estimates section below. The headline EBITDA loss of £2.2m was greater than that of FY2017E which saw a loss of £1.2m. Adjusted for restructuring, acquisition related costs, share option expenses and FX the normalised EBITDA loss came in at £1.6m.

The Group invested in its infrastructure in FY2018A resulting in an increase in operating costs from £1.7 FY2017A to £2.5m in FY2018A. The increased spend was driven by an expansion of the Group's Birmingham office as well as office relocation costs in London head count investment as well as the impact of acquisitions in 2017 and 2018. The Group ended the year with £0.9m in net cash and remains debt free.

FY2018A

PROFIT & LOSS	FY-17A	FY-18A	% Var
Revenue	2.7	3.0	10%
Adj EBITDA	(1.2)	(1.6)	-23%
Adj EBIT	(1.6)	(1.9)	-16%
Reported PBT	(1.7)	(2.5)	-34%
Fully adj PBT	(1.7)	(1.7)	2%
NOPAT	(1.6)	(1.7)	-5%
Reported EPS (p)	(1.5)	(1.6)	-3%
Fully adj EPS (p)	(1.5)	(0.6)	136%

Source: Falanx Group

The Group's customer base has increased to over 330 from 118 by organic wins and acquisitions. The number of larger accounts (>£0.1m) has grown and these factors have helped reduce customer concentration risk with the largest customer representing less than 5% of enlarged Group Revenue in 2018. In addition, monthly recurring revenue increased to £190k per month in FY2018A versus £146k per month in the prior year. This has since further increased to £240k per month.

Innovation costs of £0.5m were capitalised in FY2018A supporting further product enhancements and other software developments. In addition, a major restructuring of the Cyber sales team in the second half of the year resulted in a further £0.23m of cost that has been eliminated. Period end contracted future revenue improved to £3.0 at the end of 2018A versus that at the end of 2017A at £1.8m providing greater visibility.

Estimates

For 2019E we estimate revenue of £7.1m driven by Cyber where we estimate c.23% growth on the 2018A base revenue of £3.0m to £3.7m. In addition, we include a full year contribution from First Base of £2.4m which assumes 25% growth on its base revenue of £1.9m. Additionally, we assume £0.5m from cross-selling of MidGARD into the First Base customer base. Lastly, we include £0.5m from c. 8 months of SecureStorm ownership. For 2020E we estimate group revenue of £9.3m, 31% increase year on year with Cyber continuing to be the driver of growth driven by both organic growth and further cross selling opportunities across the enlarged customer base. We expect that recurring contract wins in 2019 will support 2020 recognitions given the low incidence of historic churn.

Estimates

Estimates	FY-19E	FY-20E
Revenue	7.1	9.3
Adj EBITDA	0.2	1.0
Adj EBIT	(0.2)	0.6
Reported PBT	(0.3)	0.6
Fully Adj PBT	0.1	0.9
NOPAT	0.1	0.9
Reported EPS (p)	(0.1)	0.2
Fully adj EPS (p)	0.0	0.3
Cash & equivalents	0.4	2.0

Source: Progressive Research

We estimate a group gross profit margin of .48% for 2019E and c. 51% in 2020E up from c. 32% in 2018A. We estimate central cost of £3.20m in 2019E which is a 39% year on year increase as the Group absorbs the additional operating costs of the acquired businesses. In 2020E we estimate total operating costs for sales, marketing and infrastructure at £3.8m of which c. £1.2m is for corporate and central functions.

We forecast the Group to move to positive adj. EBITDA position of £0.2m in 2019E from a loss in 2018A. We forecast adj. EBITDA for 2020E of £1.0m We estimate £0.5m in software development for both 2019E and 2020E, but it should be noted we make no revenue or profit assumptions in the forecast period for incremental development work the Group is currently carrying out. We estimate cash & cash equivalents of £0.7m in 2019E and £2.1m in 2020E.

We make no future assumptions for M&A and base our estimates on the Group as it currently stands. For further detail please see the Financial Summary on page 31.

Sensitivity Analysis

Given the positive market backdrop within which Falanx is operating, coupled with the Group's significant cross selling opportunities as result of its recent acquisitions and its scalability, we include a sensitivity analysis below to highlight the gearing of the group if it were to achieve a more positive revenue outcome than we are currently forecasting

Sensitivity Analysis

	Estimates	FY-19E	FY-20E
Base	Revenue	7.1	9.3
	Adj EBITDA	0.2	1.0
	EBITDA Margin	2%	10%
	Fully Adj PBT	0.1	0.9
10%	Revenue	7.8	10.3
	Adj EBITDA	0.5	1.4
	EBITDA Margin	6%	14%
	Fully Adj PBT	0.4	1.4
20%	Revenue	8.5	11.2
	Adj EBITDA	0.8	1.9
	EBITDA Margin	10%	17%
	Fully Adj PBT	0.8	1.8

Source: Progressive Research

We have constructed two upside scenarios based on a 10% and 20% uplift in revenue. We applied the same gross margin central which we employ in our base forecast across both years in both scenarios. In addition, we utilise the same central costs as the base forecast in both scenarios as we believe the Group is currently running with a central cost base which can accommodate materially high levels of revenue.

The exhibit above highlights the effects of a 10% and 20%, increase in revenue. Such increases have a high drop through rate resulting in a significant positive effect on adj. EBITDA as can be seen in the increases in EBITDA margin within the two scenarios.

Board of Directors

Mike Read Chairman and CEO

Mike has held board and senior management level positions within a number of organisations both within the US and UK. He served as Board member and CEO of AIM listed Pipex Communications Plc and President and Board member of Onemain.com, a NASDAQ listed company. He has specific expertise of creating shareholder value by executing large scale build and buy 'Roll Up' strategies. He built Onemain to be the 4th largest independent US ISP with 1 million customers. Using the same strategy, he built Pipex (broadband) to over 1 million customers and significantly increased the value of Host Europe, the Data Centre and managed services business

John Blamire – COO and Founder

John is a former officer in the British Army, having served for 10 years in Europe, Middle East and Americas gaining a wealth of operational experience in challenging circumstances and environments. After leaving the Army he co-founded Praetorian Protection Ltd, a company providing specialist security services to clients around the globe. He went on to found Falanx in 2012, leading the IPO of Falanx Group in June 2013 and the acquisition of Stirling Assynt. He repositioned Falanx group into the Cyber Security market in 2015 to take advantage of the growth opportunity, raising over £12m of growth capital during since IPO

Ian Selby - CFO (appointed Jan 2018)

Ian is a Chartered Accountant with significant experience in the software, technology and business services sectors. He was previously CFO of AIM listed Corero plc, Turnaround CFO at Zenith Hygiene Group plc, and most recently was CFO of Westminster Group plc. His earlier career included roles in NASDAQ and UK listed software companies. He has acted as a consultant to several businesses, including a buy and build MBI team operating in the business services sector where he supported the due diligence and deal structuring process. He has extensive capital markets experience (equity, debt and mezzanine), acquisition structuring, due diligence, acquisition integration as well as commercial support to the business and operational financial management

Emma Jane Shaw – Non-Executive Director

Emma is the Managing Director of Esoteric Ltd, an Electronic Sweeping, Counter-Espionage and Intelligence gathering company based in Woking, Surrey. The company is accredited by the National Security Inspectorate and provides a solution-based approach to countering espionage activity and electronic countermeasures to both commercial and non-commercial organisations internationally. An MBA graduate, and a Chartered Security Professional (CSyP) Emma's early career was spent with the Royal Military Police, followed by a career in the Ministry of Defence. Emma founded Esoteric Ltd in 1998. Emma is also the Chairman and Fellow of the Security Institute; a Board member of the Defence Industry Security Association (DISA); a Fellow of the Chartered Management Institute and a member of the Advisory Council for CSARN. Emma is also the 2012 recipient of the "Security Consultant of the Year Award" awarded by the Security Excellence Awards in October 2012.

Key Management

Richard Morrell – Chief Technology Officer

Richard is Group CTO of Falanx Group. He is best known as a twenty plus year contributor to the Linux kernel and the Open Source community, and as co-author of SmoothWall, protecting major retail brands from Ford to Halfords, Moto Service Stations

to schools, colleges and government departments in the UK and across the US. He joined Falanx from Gartner where he served as Director and CTO within their Global Security Practice. Prior to Gartner, he headed up security strategy in the US for Red Hat the leader in Open Source where he served more than 10 years in two stints, seeing the business grow to $3bn revenue from $200k.

He also serves as a director and active board member of the Cloud Security Alliance the world's largest most vocal security body in Cloud. He is a lead director of the Linux Professional Institute founding their mentoring platform and serves as an advisor to the board of the Open Source Entrepreneur Network. In downtime, he hosts one of the most listened to security podcasts on iTunes and is security editor for The Stack. He is a UK GCHQ certified security specialist to CLAS level, advising government in the UK and working on cross government projects in the US and UK for the UK MoD/US DoD and the US IRS/Office of the Executive Branch. He is an in-demand speaker and panellist at security events and has talked for NCSC and UK Government/US Department of Homeland Security in 2017 at major events

Charles Hollis – Managing Director Assynt

Charles joined Falanx Assynt as Managing Director in July 2017.

After graduating from Oxford with a Degree in PPE, Charles spent fourteen years serving at home and overseas with the British Foreign & Commonwealth Office. He worked in Jordan, Iraq, Saudi Arabia and Iran, as well as at the UK Mission to the United Nations in New York.

Charles left the Diplomatic Service in 1997 to study for an MBA at Columbia Business School. On graduation he joined CSFB in London to work with the UK mergers and acquisition team. In January 2005 Charles joined Kroll Associates as Head of the Middle East Practice before leaving to work independently as a consultant, advising clients with interests across the Middle East region.

In 2010, Charles accepted the role of Director General of the Middle East Association, the UK's leading business organisation for promoting trade relations with the Middle East and North Africa. He left the MEA in 2012 to take up the position of Managing Director for Middle East and North Africa in the Global Risks and Investigations Practice of FTI Consulting. In that role he led client projects on market entry, business intelligence, complex investigations and litigation support as well as political risk and government affairs issues.

Rick Flood -Chief Marketing Officer

Rick is responsible for all sales and marketing operations in the group. Before formally joining the management team in March he had been working with the for a few months and has restructured the Cyber Division's sales team which has contributed to the recent contract wins.

Rick is an experienced software and technology professional with 15 years' experience of cloud and SaaS technology. He originally qualified as an accountant but then switched to the software sector and ultimately to senior executive positions in sales and marketing with UK and US listed companies. His relevant AIM experience includes roles at Earthport plc, Host Europe plc and Pipex plc where he first worked with Mike Read. Rick specialises in go to market strategies & execution, turnaround and driving sales and marketing execution

Risks

Risks

Risks	Risk/ Impact	Management Action/Comment
Technology Risk	Information Technology developments move at a rapid pace. The Group's main services are based on maintaining knowledge of changing technologies and threats. The inability to keep up with such developments could result in services to clients lacking robustness	Falanx seeks to be at the forefront of change by employing best in class developers and analysts, who are continually developing applications and services that cutting/bleeding edge. In addition, it seeks M&A opportunites which augment its technologies.
Key Staff Risk	The departure of certain key staff could negatively impact the group.	Falanx has employee incentive programs such as share ownership to assist in the retention of staff. In order to manage the risk of key staff departure the group has succession plans in place.
Reputational Risk	Security breaches could damage the Group's reputation and status as a trusted advisor resulting in damage to its ability to maintain and win client work.	The group employs stringent security protocols within its own infrastructure to ensure a the highest levels of security and adherance to industry accreditations and standards
M&A risk	The Group is actively pursuing a stated M&A strategy. Failure to complete detailed due diligence on an acquisition or appropriately integrate or monitor aquired assets could lead to a destruction of value for shareholders	Falanx performs extensive due dillegence on targets prior to acqusition. The senior manangement team have an extensive history of acquiring and integrating acquistions into a parent company.
Market Risk	The Group is a public ally listed company whose shares are exposure to the inherent risk associated with being a plc.	The management of Falanx actively seeks to educate potential investors on the Group and its activities and financial well being. The creation of such transparency seeks to support the appropriate assignment of value to the compaany.
Financial Risk	The Group has financial risks which include liquidity risk, credit risk and foreign currency risk that arise as part of its normal course of operations.	A risk management program has been established to protect the compant against the potential adverse effects of these financial risks.
Political Uncertainty	Brexit and other political tensions globally	The directors monitor emerging news and trends and remain alert to any potential impact on the trading of the group.

Source: Falanx Group, Progressive Research

Appendix

Testing Services

Testing Services

Service	Segment	Description
Website and application penetration testing	General Security	The testing of applications with the use of automated software and heavily reliant upon a seasoned analyst that simulates an opportunistic attack to identify vulnerabilities typically associated with misconfiguration (SSL/tLS testing, backup and unreferenced files, admin interfaces, HTTP methods), data validation (cross site scripting, SQL injection), business logic (shopping cart, payment transactions, etc),session management (cookie attributes, cross-site request forgery) authentication defects and privilege escalation. Review of web server configurations are undertaken. The Methodology is informed by the Open Web Application Security Project (OWASP), ISO 27001,
Web services testing	General Security	Testing includes information gathering, configuration management, WSDL testing which attempts to discover entry point to retrieve sensitive information, XML structural testing, XML content testing, HTTP GET/REST testing, SOAP attachment testing, replay testing (impersonation of valid users of the system), server configuration
External infrastructure & Firewall testing	General Security	Firewall rules testing, network topology review and testing, firewall and VPN pentration, configuration error testing including vendor defaults, remotely accessible internal services
Onsite network penetration testing	General Security	Testing includes a mapping of network and structure, target sensitive information (payroll, personal data, financial information), review workstation and server configurations, Intrusion Detection and Prevention (IDS/IPS) testing, social engineering (staff education), remote access and VPN testing.
Wireless penetration testing	General Security	Testing attempts to identify access points and evaluate the security of such points, analysis traffic and devices on network, interception of encrypted data and methods of authentication.
Mobile application testing	General Security	A layered approach to testing is taken addressing application functionality, interaction with the device operating system and remote services such as web services and social media. Testing includes information gathering (workflow, traffic analysis, secure protocol checks, API), application analysis (permissioning, configuration errors, entry point for untrusted data), authentication (replay attacks, brute force attacks, touch passwords/swipes, push notification and SMS, single sign on functionality, session management (time outs, sensitive information flushed out on session expiration), authorisation (privilege escalation, path traversal, licensing security), Data Storage (encryption services exposed APIs, sandboxed locations), Transport Layer protection (certificate pinning and validation, encryption transaction each layer), Information disclosure (sensitive information to shared logs, data leakage, third party libraries), Client side injection (potential data injection attack vectors)
Laptop testing – testing and tracking.	General Security	Service includes conduct testing of laptop build, assess client security controls, break out testing, subvert operating system during boot up, attempt to reset local windows and system user account passwords, access protected and stored information by analysing hibernation files, cold boot attack to retrieve encryption keys from memeory, attempt physical memory manipulation, workstation testing as well as scripting of policies and procedures.
Cloud security testing	General Security	The testing of the most popular providers including Amazon SWS, Microsoft Azure and Rackspace. Flanax tests identity and acess management, OS-Level management and security, encryption, logging and configuration, access polies and system interplays for key management.
SharePoint configuration security review – configuration and server hardening.	General Security	Assessment of indentity and access management, installation and configuration, central administration, site administration, backup and recovery, logging and reporting and extensions.
General Data Protection Regulation (GDPR) testing,	Compliance Testing	Assist in creating process and procedure for regular testing of data processes, assessing and evaluating the effectiveness of technical and operational procedures. The Group partners with Cordery to offer this service
Payment Card Industry Data Security Standard (PDI DSS)	Compliance Testing	Requirements 6.6 (review of public facing web applications) and 11.3 (internal and external pentration testing of network and application layer testing as well its controls and processes) call for penetration testing
Supply chain assessments and Outsourcer assessments.	Compliance Testing	A review of the clients outsourced partners polices and procedures and technical controls.
Cyber Essential Accreditation	Compliance Testing	Services include conduction a technical review of a clients IT systems to assess Cyber Essential accreditation.

Source: Falanx Group (Firstbase)

High Profile Attacks

Carphone Dixons reported on the 13th of June 2018 that it had been subject to an 'attempt to compromise' the data of 5.9 million customers credit cards. In addition, the attack accessed over 1.2 million records holding personal data. The Financial Times reported that the attack had been ongoing since July 2017 and was not detected for almost a year. The company has yet to quantify the loss, but on the day the company's share price was down over 6%.

Equifax, the consumer credit reporting agency, announced on 7 September 2017 that social security numbers, driver's license numbers, birth dates and addresses of up to 145m customers had been accessed. It was also believed that 209,000 customers' credit data had been accessed as well as 182,000 dispute records containing personal data. Access to the information was said to have been gained through vulnerabilities in its website software (NY Times 07.09.17) The fallout has been significant with 240 class action lawsuits filed and 60 regulatory and governmental inquiries launched into the event as of November 2017 according to Bloomberg. Equifax increased its spending on security in the wake of the attack and cost of the liability has been estimated at $110m. In addition, the company suffered loss of renewals and future business given the lack of confidence in its security procedures.

In May 2017 the NHS was significantly affected by the 'Wannacry' randsomware attack. The attack exploited a vulnerability in Microsoft windows networking protocol and using tools believed to have been developed by the NSA (US National Security Agency). A patch had been deployed for supported systems, but many users neglected to update the patch or were using unsupported older versions. The phishing attack affected more than 300,000 computers where malware infiltrated NHS computers, locking (encrypting) its files with the attackers then demanding bitcoin payment to release the files. Fed-ex, Telefonica and Deutsche Bahn were all affected in this attack.

Maersk was the target of the NotPetya ransomware attack which is said to have cost the firm $300m in 2017. The Group was forced to halt operations in 76 port terminals globally for several days as it tried to come to grips with the attack. Regarding the attack Maersk CEO was quoted as saying. " Most business problems you have an intuitive idea what to do. But with this and my skills, I had no intuitive idea how to move forward." (theregister.co.uk). This quote underlines how unprepared many senior executives are against the cyber threats their businesses face. The malware is said to have surfaced post a malicious update to the Ukraine's most popular accounting software MeDoc. Accounting software often requires location administration rights, which appears to be the vulnerability exploited in this attack.

Yahoo experienced two attacks in which 500m users accounts had been accessed in 2014 and more 1bn accounts compromised in 2013, where sensitive information as well as encrypted passwords and security questions were accessed. The attacks were not uncovered by Yahoo but were addressed after the attacks were brought forward by law enforcement officials. Yahoo suffered serious reputational damage at sensitive period as it was undergoing extensive leadership changes as well as growth challenges.

Talk Talk was the subject of a large attack in 2015 where the personal data of 157,000 customers was accessed by hackers. As a result of the attack Talk Talk was fined £500,000 by the Information Commissioner's Office (ICO). Post mortem analysis suggests that hackers were able to access Talk Talk's network through an insecure website it acquired from Tiscali.

Global Cyber Security Providers

Competitors

Company	Description	Company	Description
Accenture	Accenture is a global management consulting and professional services firm. Its Cyber division focuses on cyber defence, digital identity and compliance	Masergy	Provides MDR services for organisations globally
ATSO SE	Atos is a global leader in digital transformation. Its cyber division specialises in prevention, detection and remediation services	Morphick	Provides MDR services in an enterprise platform
ATT Cyber Security Services	Part of AT&T its focus is to dectect, deter and reduce network disruptions and damage due to cyber attack	NCC Group	Provider of software escrow, cyber security and web performance services
Axial	VAR founded in 1989	N-Dimension	MDR for NCI providers (gas, water and power companies).
BAE Applied Intelligence	Division of BAE systems	Nettitude	Founded in 2003 as a VAR but has expanded offering
BT Security	A division of BT. Focuses onDistributed denial of service attacks as well as cloud, firewall, email service among others	NTT Security	MSSP which provides solutions for both on premise and cloud technology
Cap Gemini	Global consulting firm. Its cyber capabilities offers a managed mulit-teneted security operations centre (SOC) and security information and event management (SIEM)	Optiv	Provider of several SOCs which offer continuous MDR services
Century Link	Offer theat prevention, inndicent repsonse and analysis services	Orange Business Services	Division of telecom provide Ornage which provides MDR services on a continuous basis
CGI	Independent information technology and business process services firms which offer 10 SOCs globally	Proficio	Provides co-managed and custom built services including 24/7 MDR
Cipher	Offers SOC services globally	Quann Security	Division of Certis Cisco. Largest provider of certified SOCs in Asia Pacific
CNS Group	Founded in 1999 orginally with public sector and financial services focus	Raytheon Cyber	Division of Raytheon. Provides MSSP services for US federal agencies and larg corporations
CSS Corp	MSSP focused on IoT globally. IoT assessments and implemenation of controls	root9B	Provider of cyber security and advanced technology training capabilities, operational support and consulting services
Delta Risk	Provides continuous montoring of a clients local and/or cloud assets	SecureData	Professional Services provider founded in 1992
DXC Technology	Provides services to protect crtical data and systems	SecureLink	Beligian headquarteres MSSP.
ECS	Division of an IT services Group	SecureWorks	Intelligence driven MSSP. Providing services to large and small enterprises globally.
ECSC	Managed sercurity service provider	Securiry On-Demand	US based MSSP providing managed network, endpoint and application security services
EY Cybersecurity	A division of Ernst & Young which provices MSSP services which included MDR	SecuVail	MSSP Headquartered in Japan it provides cyber services and log analysis services locally
General Dynamics Information Technology	A division of GD providing cyber sercurity services such as prevention, resilliance, training and analystics amoung others	Sword & Shield	US based MSSP focusing on SMEs. Provides MDR services.
GM Security Technology	A MSSP focused on Latin America and Puerto Rico, providing incident response and replication centres	Symantec	Provides security products and solutions to protect small, medium, and enterprise businesses from advanced threats, malware, and other cyber attacks. Its brands include Norton, LifeLock, DigiCert, and ID analytics.
GRC International	Founded in 2002 as Information Security book publisher	Tata Consultancy	Consultancy provider of SOC services, dection and respsonse.
HCL	Technology and outsourcing company which provide MDR services thorugh tis 4 global SOCs	Trustwave	MSSP for threat, vulnerabilty and compliacne management
Herjavec Group	MSSP specialising in complex multi technology environments	Unisys	MSSP focused on advance cyber threats and attacks.
IBM Security	IBM security develops intelligent enterprise security solutions and service to assist corporations globally	Verizon Enterprise	Division of Verizon telecom. Runs 9 SOCs across 4 continents.
Inteli Secure	MSSP which provides Critcal assest protection , SOC and incident response	Vigilant	MSSP focused on SMEs providing managed network serviced and monitoring
Kudelski Security	MSSP for public sector and large enterprises. Operates next generation SOCs (Cyber Fusion Centres)	Wipro	Provides IT Services, Business and Technology Consulting and outsourcing. Provides monitoring, vulnerability and compliance management among other cyber services

Source: Progressive Research, cybersecurityventures.com

Glossary

Glossary

Glossary	
Red Team	A red team or the red team is an independent group that challenges an organization to improve its effectiveness by assuming an adversarial role or point of view. It is particularly effective in organizations with strong cultures and fixed ways of approaching problems.
VPN	Virtual Private network
Phising	Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. (WIKI)
API	An application programming interface is a set of subroutine definitions, protocols, and tools for building application software. In general terms, it is a set of clearly defined methods of communication between various software components
GPG13	Good Practice Guide - UK government recommended set of people and business processes and technology to improve company risk profiles.
SC Clearance	SC Clearance is a mandatory check designed for people working within the Government or private sectors whom handle or come into contact with secret/sensitive information.
DV Clearance	Developed Vetting, is the most extensive form of UK security vetting and is very thorough, including checks of your identity documents and employment and education references
Vishing	Vishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity over the phone
metadata	data that provides information about other data". Three distinct types of metadata exist: descriptive metadata, structural metadata, and administrative metadata (wiki)
machine learning	Machine learning is a subset of artificial intelligence that often uses statistical techniques to give computers the ability to "learn" with data, without being explicitly programmed. Learning is developed through exposure to new scenarios, testing and adaptation, while employing pattern and trend detection for improved decisions in subsequent (though not identical) situations . (Wiki/Techopedia)
Software as a Service	SaaS applications aren't sold as software packages for download or purchase, users don't buy licenses or upgrades. Instead, they pay a flat, usually monthly, subscription fee.
Manages Services	The comprehensive outsourcing of information technology business functions, such as security and networking,. MSP's are retained to run the software and to run maintenance and install upgrades and, depending on the model, to host applications

Source: Progressive Research

Financial Summary: Falanx Group

Year end: March (£m unless shown)

PROFIT & LOSS	2016	2017	2018A	2019E	2020E
Revenue	1.8	2.7	3.0	7.1	9.3
Adj EBITDA	(2.3)	(1.2)	(1.6)	0.2	1.0
Adj EBIT	(2.3)	(1.3)	(1.7)	0.1	0.9
Reported PBT	(2.6)	(1.7)	(2.5)	(0.3)	0.6
Fully Adj PBT	(2.6)	(1.7)	(1.7)	0.1	0.9
NOPAT	(2.6)	(1.6)	(1.7)	0.1	0.9
Reported EPS (p)	(3.8)	(1.5)	(1.6)	(0.1)	0.2
Fully Adj EPS (p)	(3.8)	(1.5)	(0.6)	0.0	0.3
Dividend per share (p)	0.0	0.0	0.0	0.0	0.0

CASH FLOW & BALANCE SHEET	2016	2017	2018A	2019E	2020E
Operating cash flow	(1.9)	(1.3)	(2.1)	0.5	2.0
Free Cash flow	(1.9)	(1.8)	(5.9)	(0.2)	1.4
FCF per share (p)	(2.8)	(1.6)	(3.6)	(0.1)	0.8
Acquisitions	(0.5)	(0.1)	0.0	(0.1)	0.0
Disposals	0.0	0.0	0.0	0.0	0.0
Shares issued	2.5	1.8	6.3	0.1	0.0
Net cash flow	0.0	(0.3)	0.5	(0.2)	1.4
Overdrafts / borrowings	0.0	0.0	0.0	0.0	0.0
Cash & equivalents	0.4	0.4	0.9	0.7	2.1
Net (Debt)/Cash	0.4	0.4	0.9	0.7	2.1

NAV AND RETURNS	2016	2017	2018A	2019E	2020E
Net asset value	0.4	0.8	4.7	4.5	5.1
NAV/share (p)	0.6	0.7	2.9	2.8	3.1
Net Tangible Asset Value	0.1	0.1	0.1	0.2	0.2
NTAV/share (p)	0.1	0.1	0.1	0.1	0.1
Average equity	0.2	0.6	2.8	4.6	4.8
Post-tax ROE (%)	(769.3%)	(266.8%)	3.3%	19.2%	0.0%

METRICS	2016	2017	2018A	2019E	2020E
Revenue growth		51.1%	10.1%	134.8%	31.5%
Adj EBITDA growth		(47.1%)	30.1%	1,034.1%	466.3%
Adj EBIT growth		(45.8%)	30.8%	1,919.8%	877.2%
Adj PBT growth		(36.1%)	(1.8%)	1,922.3%	877.2%
Adj EPS growth		(60.5%)	(57.6%)	1,937.9%	904.7%
Dividend growth		N/A	N/A	N/A	N/A
Adj EBIT margins		(46.1%)	(54.8%)	1.3%	9.5%

VALUATION	2016	2017	2018A	2019E	2020E
EV/Sales (x)	6.9	4.5	4.1	1.8	1.3
EV/EBITDA (x)	(5.4)	(10.2)	(7.8)	73.1	12.9
EV/NOPAT (x)	(4.7)	(7.9)	(7.5)	136.8	14.0
PER (x)	N/A	N/A	N/A	146.9	14.6
Dividend yield	N/A	N/A	N/A	N/A	N/A
FCF yield	(54.8%)	(31.2%)	(71.4%)	(2.0%)	16.4%

Source: Company information and Progressive Equity Research estimates

Disclaimers and Disclosures

 PERL provides professional equity research services, and the companies researched pay a fee in order for this research to be made available. This report has been commissioned by the subject company and prepared and issued by PERL for publication in the United Kingdom only. All information used in the publication of this report has been compiled from publicly available sources that are believed to be reliable; however, PERL does not guarantee the accuracy or completeness of this report. Opinions contained in this report represent those of the research department of PERL at the time of publication, and any estimates are those of PERL and not of the companies concerned unless specifically sourced otherwise. PERL is authorised and regulated by the Financial Conduct Authority (FCA) of the United Kingdom (registration number 697355).

This document is provided for information purposes only, and is not a solicitation or inducement to buy, sell, subscribe, or underwrite securities or units. Investors should seek advice from an Independent Financial Adviser or regulated stockbroker before making any investment decisions. PERL does not make investment recommendations. Any valuation given in a research note is the theoretical result of a study of a range of possible outcomes, and not a forecast of a likely share price. PERL does not undertake to provide updates to any opinions or views expressed in this document.

This document has not been approved for the purposes of Section 21(2) of the Financial Services & Markets Act 2000 of the United Kingdom. It has not been prepared in accordance with the legal requirements designed to promote the independence of investment research. It is not subject to any prohibition on dealing ahead of the dissemination of investment research.

PERL does not hold any positions in the securities mentioned in this report. However, PERL's directors, officers, employees and contractors may have a position in any or related securities mentioned in this report. PERL or its affiliates may perform services or solicit business from any of the companies mentioned in this report.

The value of securities mentioned in this report can fall as well as rise and may be subject to large and sudden swings. In addition, the level of marketability of the shares mentioned in this report may result in significant trading spreads and sometimes may lead to difficulties in opening and/or closing positions. It may be difficult to obtain accurate information about the value of securities mentioned in this report. Past performance is not necessarily a guide to future performance.