WHITEHAWK®

WHITEHAWK CEC INC.

The following report has been commissioned and paid for by WhiteHawk Ltd (Company) and has been prepared by Pitt Street Research, an Authorised Representative of BR Securities Australia Pty Ltd. The report solely reflects the views of Pitt Street Research.

Any opinions, forecasts, recommendations or forward-looking statements in the report reflect the judgement and assumptions of Pitt Street Research at the date of publication of the report. The Company does not endorse the findings or contents of the report, including any price target, earnings forecast or other statement about the Company's prospects, and will not be responsible for any loss or damage arising in any way from errors, omissions or misstatements in the report or the use of, or reliance on, the report in any way.

PITT STREET RESEARCH

WhiteHawk Limited

Risk mitigation in the Digital Age

Share Price: A$0.051

ASX: WHK

Sector: Consumer Discretionary

14 May 2020

WhiteHawk (ASX:WHK) has developed a proprietary technology platform that focuses on identifying, prioritizing and mitigating cyber risks for Small and Medium-sized businesses (SMB) and tailored online risk platforms and programs for Enterprise and government agencies. WHK takes a pragmatic and scalable approach to cyber risk by partnering and integrating best of breed publicly available data and analytics' Software as a Service (SaaS) subscriptions. Its added value lies in optimizing a breadth of cyber risk data sets and producing Cyber Risk Scorecards an action plan that can be easily and affordably implemented by any company. Mitigation of cyber risks is largely done through third-party solutions that WHK vets and sells to customers in a revenue sharing agreement with the vendors, similar to the Apple App Store model.

Highly scalable business model

Spending on cyber security by both the public and private sector continues to grow at a very healthy pace. The company has opened up a large addressable market in the Government and Enterprise verticals by subcontracting with larger business partners. Also, it is able to address the SMB market for cyber security through its partnership with Sontiq. Combined with its revenue sharing agreements with many cyber security providers that can sell through online Cyber Risk Marketplace, we believe WHK has developed an attractive and highly scalable business model.

Valuation of A$0.35 per share

We expect WHK will be able to strongly ramp up revenues in the next few years, at attractive and growing margins. Our blended valuation, equally weighted between DCF and EV/Sales, yields a value of A$0.35 per share base case and A$0.41 per share in a bullish scenario.

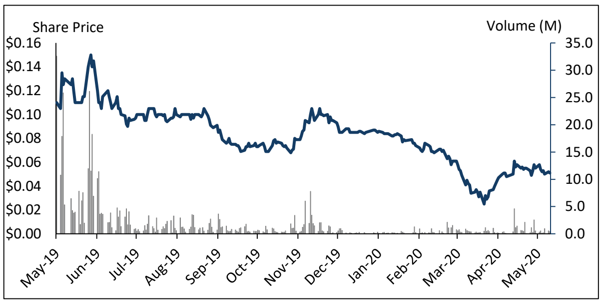
Year to Dec (AUD)[1]	2019A	2020F	2021F	2022F	2023F
Sales (m)	1.6	9.8	18.0	23.8	30.0
EBITDA (m)	(3.4)	(1.0)	(0.1)	0.9	2.1
Net Profit (m)	(4.4)	(1.5)	(0.5)	0.4	1.5
EBITDA Margin (%)	nm	nm	nm	3.7%	7.1%
RoA (%)	nm	nm	nm	3.5%	11.0%
EPS (cents)	(3.1)	(1.0)	(0.3)	0.2	1.0
EV/Sales	6.7x	0.6x	0.4x	0.3x	0.2x
EV/EBITDA	nm	nm	nm	8.3x	2.4x
P/E	nm	nm	nm	26.4x	6.3x

Source: Company, Pitt Street Research

Market Cap. (A$ m)	159.0
# shares outstanding (m)	8.1
# shares fully diluted	186.6
Market Cap Ful. Dil. (A$ m)	9.5
Free Float	64.3%
52-week high/low (A$)	0.17/0.03
Avg. 12M daily volume ('1000)	1,514.3
Website	www.whitehawk.com

Source: Company, Pitt Street Research

Share price (A$) and avg. daily volume (k, r.h.s.)



Source: Thomson, Pitt Street Research

Valuation metrics	
Fair valuation (A$)	0.35 – 0.41
WACC	12.0%
Assumed terminal growth rate	2.0%

Source: Pitt Street Research

Subscribe to our research HERE

Analysts: Marc Kennis & Cheng Ge

Tel: +61 (0)4 3483 8134

marc.kennis@pittstreetresearch.com

cheng.ge@pittstreetresearch.com

[1] Based on USD/AUD exchange rate of 0.64.

Table of Contents

Cyber risk mitigation in the Digital Age

WhiteHawk Limited (ASX:WHK) listed on the ASX on 24 January 2018, raising A$4.5m in the IPO process. The company has developed a technology platform that focuses on identifying, prioritizing and mitigating cyber risks for Small and Medium-sized businesses (SMB) as well and tailored online risk platforms and programs for Enterprise and government agencies (Figure 1).

Figure 1: WhiteHawk Cyber Risk assessment and mitigation model

Source: Company, Pitt Street Research

WHK is currently selling and tendering to multiple branches of the United States (US) government, including the Department of Homeland Security (DHS). The US Defence Industrial base (DIB), i.e. companies involved in the US defence industry, is another key target market for WHK. Additionally, Financial Services companies, such as banks and financial firms, and companies in the manufacturing sector are key commercial targets for the company.

Cyber Risk Marketplace for the SMB segment

Specifically for the SMB segment, WHK has established the world's first online Cyber Security Exchange, enabling smaller companies to source relevant cyber security tools without having to retain expensive consultants or having to establish large scale cyber security programs.

Through online questionnaires and assessments, companies can get an elaborate picture of where their cyber risks lie in categories such as data leak prevention, malware, denial of service mitigation, mobile data security, network intrusion detection, traffic analysis, vulnerability assessment, encrypted communications and access control.

They can subsequently purchase remediation tools on WHK's marketplace through attractive SaaS (Software-as-a-Service) subscription models.

Attractive revenue sharing model

WHK sources these remediation tools from third-party vendors and clips the ticket on every monthly subscription payment, i.e. between 10% and 20% of the gross revenue.

These tools are sold in three bundles;

- **Basic**, providing basic cyber security at an average price between US$1,000 and US$2,000 per year, depending on the number of employees.
- **Balanced**, which provides more elaborate cyber security at an average price of US$5,000 per year, and
- **Advanced**, which provides best-of-breed cyber security for all required categories. Advanced costs US$10,000 per year on average.

Servicing larger customers through two main offerings

WHK's online approach to determining key cyber risks is also well-suited to larger organisations. Through a Cyber Threat Readiness Questionnaire and, if necessary, a cyber risk assessment, the company can match tailored risk mitigation solutions to companies and organizations based on current threat trends.

WHK's cyber risks assessment model is offered to larger organisations through two service models, i.e. Cyber Risk Program and Cyber Risk Radar.

Cyber Risk Program

Through the Cyber Risk Program, WHK offers mid-sized to large clients an independent expert approach to monitor, identify, prioritize, validate and mitigate cyber risks to their operations, revenue and reputation (Figure 2).

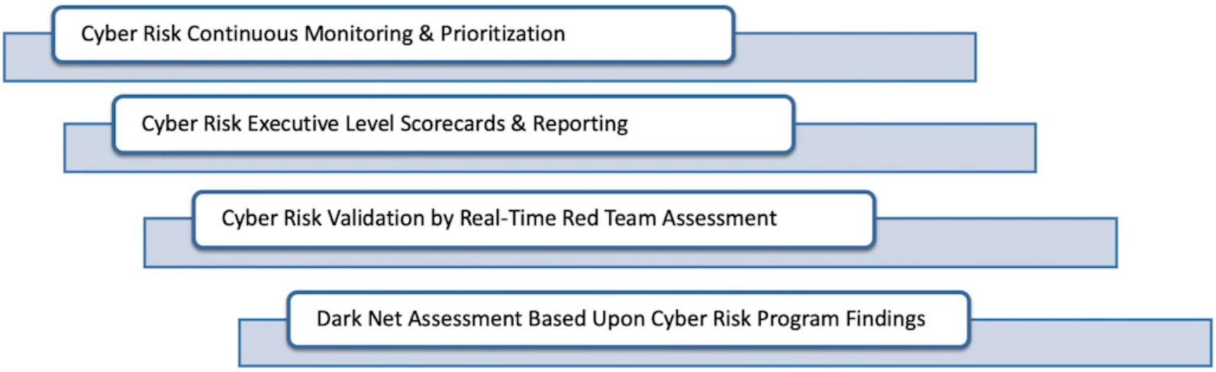
WHK will look at a customer from the outside in, i.e. from a "bad guys" point of view, and assess an organisation's network security, data security, its operations etc. Feedback and findings are presented to the organisation through Cyber Risk Score Card reports, to include appropriate remediation options.

Covering ~75% of all cyber security risks

Cyber Risk Program is not designed to offer 100% security, but rather to improve security from a level of 20% to 30%, which is where most organisations are, to around 75% of all cyber security risks covered.

The program can be implemented very fast and as such provides a very pragmatic solution for organisations to substantially improve their cyber security within weeks.

Figure 2: Cyber Risk Program service features



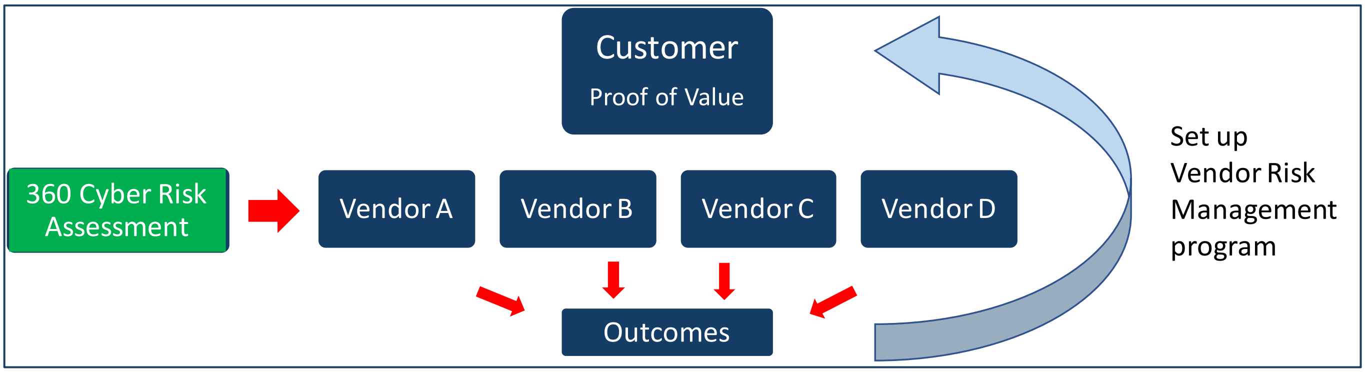
Source: Company, Pitt Street Research

Cyber Risk Radar

In addition to assessing cyber security risks within a customer's own organisation, WHK can also perform a cyber risk assessment on a customer's broader environment, including its supply chain. Cyber Risk Radar will perform cyber risk identification at external parties and subsequently offer options for mitigation and remediation, i.e. best-of-breed, third-party solutions in a SaaS subscription model.

In the case of a supply chain assessment, a select number of vendors will be assessed initially. Based on WHK's feedback, customers can subsequently develop a Vendor Risk Assessment program that can then be deployed across their entire supply chain (Figure 3).

Figure 3: Cyber Risk Radar for an organisation's supply chain



Source: Company, Pitt Street Research

Cyber Risk Radar and Program offered at different service levels

WHK offers Cyber Risk Radar at different service levels

Cyber Risk Radar and Cyber Risk Program are mainly geared to the Enterprise market. The 1st level of service can include a one-time delivery of a Cyber Risk Scorecard or consultancy work, e.g. to establish a customer's cyber risk status or cyber risk in its supply chain. This first level of assessment services is typically a steppingstone to a broader service offering from WHK.

WHK's 2nd level of services includes annual subscriptions that include Cyber Scorecards, Cyber Risk Portfolio Reports and ongoing consultancy around cyber risks. The 3rd level of services adds deeper analysis of ongoing business risks and a broad view of the cyber risk landscape.

Engaging with large organisations through prime contractors

When it comes to engaging with larger organisations, including US government agencies, such as the Department for Homeland Security (DHS), WHK can work directly with prospective customers. However, WHK mostly engages through subcontractor roles with large and established prime contractors. The prime contractor will manage the tender and WHK will be part of that tender, working through pilot projects, proofs-of-concept (POC) and proofs-of-value (POV) to transition to an enduring service or program.

Sontiq partnership substantially expands SME marketing power

In March 2019, WHK announced a partnership with Sontiq, formerly known as EZShield. Sontiq specializes in identity theft protection and mobile cyber security and has more than 27 million customers in the US.

Combining both companies' expertise expands marketing power

The partnership brought together WHK's expertise in cyber risk profiling and Sontiq's product offering around identity theft, financial fraud protection and mobile cyber security services. It leverages both companies' expertise and substantially expands each individual company's marketing capabilities.

WHK's cyber risk solution has been integrated into Sontiq's Small Business Suite. This integrated Digital Age Business Risk Suite combines functionality in several areas in one platform. Cyber security functionality includes identity theft, financial fraud, mobile security, threats from the dark net with respect to data theft and cyber risk services. Pricing is around US$1,100/year for companies with up to 15 employees.

Based on customers' answers to non-technical questions in the online questionnaire, WHK's platform provides individual product and service options available in its Cyber Risk Marketplace.

Also targeting wholesale deals with banks and Managed Service Providers

Sontiq and WHK are also aiming to sell this Digital Age Business Risk Suite in a wholesale format to financial institutions and managed service providers (MSPs). In this model, WHK sells cyber security bundles to banks and MSPs at wholesale prices in a SaaS subscription model. A bank or MSP could subsequently offer these bundles of cyber security products to their customers, e.g. a bank's small business customers as a market differentiator.

Wholesale deals could become quite substantial for WHK

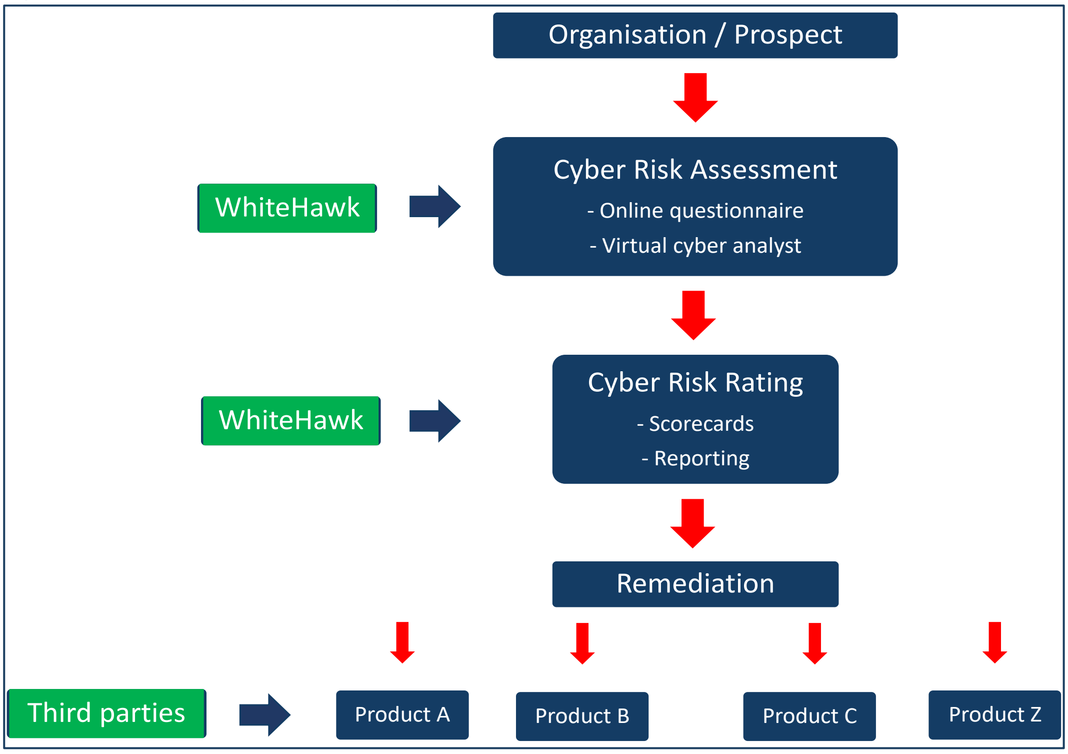
How these banks and MSPs charge their business customers is not relevant for WHK. The company would simply sell x number of bundles at wholesale prices, so these deals could be quite substantial for WHK, i.e. a bank could offer a bundle to many thousands of small business clients simultaneously. Alternatively, a bank or MSP could roll out a certain bundle across all its SME customers at no cost. WHK could potentially also simply charge a lump sum per bank or MSP per year, assuming certain levels of take up by their respective customers.

WHK is currently in discussions with multiple financial institutions and MSPs. Given the large size of most of these organisations, closing such Enterprise deals typically takes between 6 and 18 months.

WHK's secret sauce is its proprietary assessment model

WHK hasn't reinvented the wheel when it comes to cyber risk mitigation, e.g. by developing new software for certain, specific cyber risks. Rather, when it comes to the company's edge in the marketplace, its added value lies in its proprietary algorithms and analysis tools used in the initial online assessments of companies' cyber risks (Figure 4).

Figure 4: WhiteHawk proprietary algorithms and analysis tools used in initial assessments



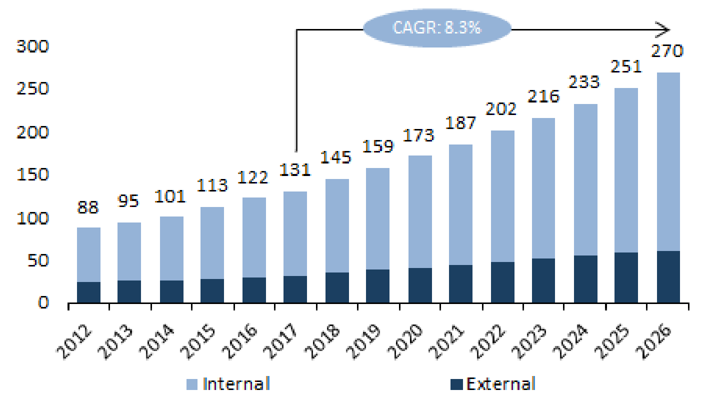
Source: Pitt Street Research

There is currently no alternative to WHK's online, largely automated, assessment methodology, other than a much more manual, and expensive, type of cyber risk assessment, i.e. using consultants.

Global cybersecurity market is witnessing accelerated growth

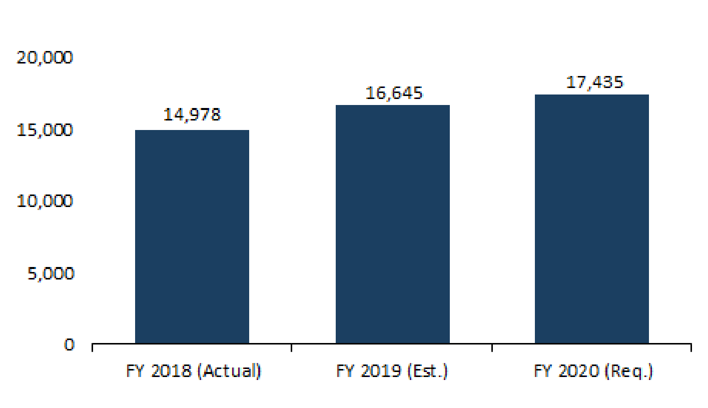
As a result of the high cost of cybercrime to businesses and government institutions alike, spend on cybersecurity is increasing. In its sector competitiveness plan (SCP), the Australian Cyber Security Growth Network estimates the global security spend to reach US$270bn by 2026 (Figure 5). In our view, this represents a substantial growth opportunity for WHK, as more organisations seek services to understand their cybersecurity needs.

Figure 5: Global cyber security spend (in US$bn)



Source: Australian Cyber Security Growth Network

Figure 6: US federal cybersecurity funding (in US$m)



Source: FY 2020 President's Budget Request

The US in particular is highly vulnerable to cybercrime, driven primarily by the digitisation of personal information (names, addresses, SSNs, etc.) in a number of institutions and driven by regulation. As per Juniper Research estimates, by 2023, half of the data breaches globally are expected to occur in the US.

US government spending on cyber security to grow strongly

Moreover, cybersecurity remains a key concern for the US government, as it directly impacts national security. With a history of state-sponsored cyber-attacks, such as the involvement of Russian hackers in the Yahoo data breach, the US government's funding for cybersecurity is expected to continue to grow strongly (Figure 6).

The CMMC will be a strong growth driver for WhiteHawk

CMMC affects ~300,000 companies in the DoD's supply chain

When it comes to cybersecurity, the US Department of Defence (DoD) has particularly stringent requirements. To this extent, DoD released the Cybersecurity Maturity Model Certification (CMMC) standard in January 2020. Through this unified standard, the DoD aims to implement strict cybersecurity measures across the Defence Industrial Base, which comprises of more than 300,000 companies in the DoD's supply chain.

With five levels of certifications (Figure 7), the CMMC is a comprehensive framework, which all aspiring DoD contractors (and subcontractors) will need to adhere to in order to work on DoD projects.

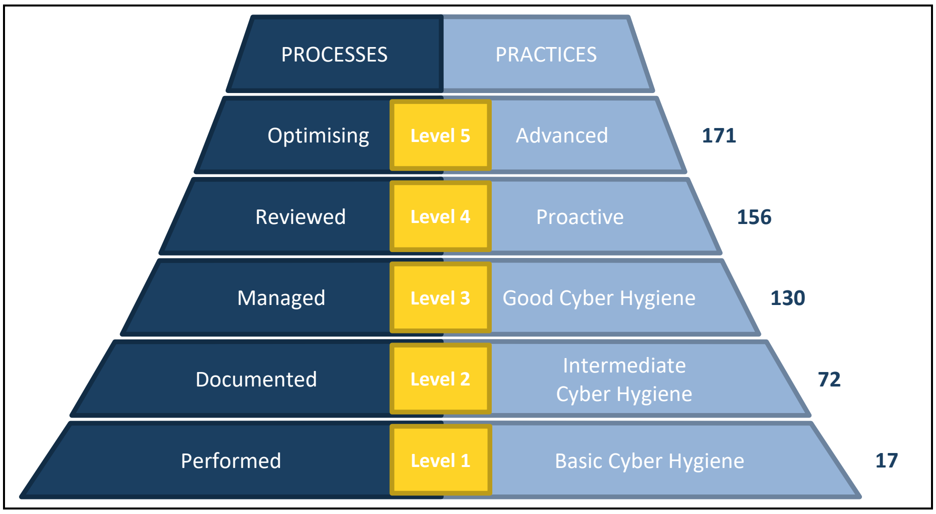
Moreover, in order to promote swift implementation, the DoD has stipulated quite a short timeframe to do it in. The department has indicated that the basic requirements for CMMC will start appearing in requests for information (RFIs) in June 2020. In our view, as contractors scramble to meet the

Contractors seeking cyber risk assessment and profiling to drive demand for WHK's services

stipulated deadline, the demand for specialised outside counsel on cybersecurity assessment and risk profile is set to increase.

We believe this presents a substantial growth opportunity for WHK. Leveraging on its experience of working with a Top 12 US DIB companies, WHK is well-positioned to establish itself as a key provider of cyber risk profiling services to current and aspiring DoD contractors.

Figure 7: CMMC levels



Source: Huntsman Security

WHK positioned in sweet spot of financial institutions' spend

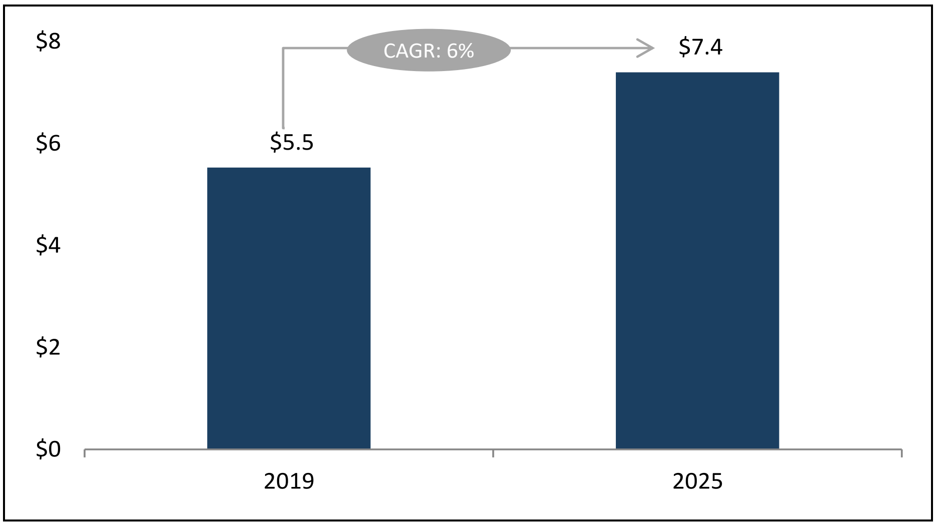
Banking and financial services institutions are often the most lucrative target sectors for cybercriminals. This is primarily because they store highly sensitive information – bank account numbers, credit card details, transaction details, etc. – of millions of customers in their servers. Access to this information is highly profitable for cybercriminals, as it can be sold on the dark web. Consequently, cybersecurity has become a key component of financial institutions' budgets.

Apart from banks, other financial service institutions, such as registered investment advisors (RIAs), are also realising the importance of cybersecurity systems. As per TD Ameritrade's '*2020 RIA Sentiment Survey*', nearly 59% of RIAs were considering investing in cybersecurity in 2019, up from just 11% in 2018.

Services account for 50% of all spending on cyber security by financial institutions

As per a recent report by Research Nester, the US financial services cybersecurity market is expected to reach US$7.4bn by 2025, growing at a CAGR of 6% over 2019–2025 (Figure 8). Notably, the report also highlighted that among the three product types in the market – hardware, software and services – the services segment holds the lion's share of revenues. Valued at roughly US$2.6bn in 2019, the services segment accounted for approximately 50% of the share of cybersecurity products for the US BFSI sector. Notably, this is where WHK operates.

Figure 8: US cybersecurity market for BFSI industry (in US$bn)



Source: Research Nester – U.S. Financial Service Cyber Security Market

Cybercriminals are also targeting Fortune 1000 companies, as well as companies in the industrial sector, primarily for ransom. Since downtime can be extremely costly for these companies, we believe they are likely to increase their spending on cybersecurity products over time.

Moreover, as industries move towards digital supply chains, the threat of cybercrimes due to weak third-party infrastructure increases exponentially. Leveraging the expertise of its Cyber Risk Scorecard and Risk Portfolio Reports, we believe WHK is well-positioned to generate substantial revenues in this domain going forward.

Cyber threat for SMBs is more real than ever

Lack of sufficient cybersecurity systems and specialised staff makes SMBs easy targets for cybercriminals. As per Continuum's 2019 *'Small Business Cyber Security Report*', 62% of SMBs lack in-house personnel to handle cybersecurity operations, while 56% do not have security specialists. This makes SMBs, which often store transaction- and customer-related information, highly vulnerable to cyber threats.

This is where WHK comes into play. In our view, as cyber threats continue to rise, this vulnerability is set to drive SMBs to seek cybersecurity advice and assistance. We believe WHK is well-positioned to benefit from this growth opportunity.

Additionally, amid the current global pandemic, as more and more people work from home, SMBs that had previously remained complacent towards cyber threats will likely seek outside counsel to strengthen their systems against potential breaches. We believe this provides another substantial growth opportunity to the company.

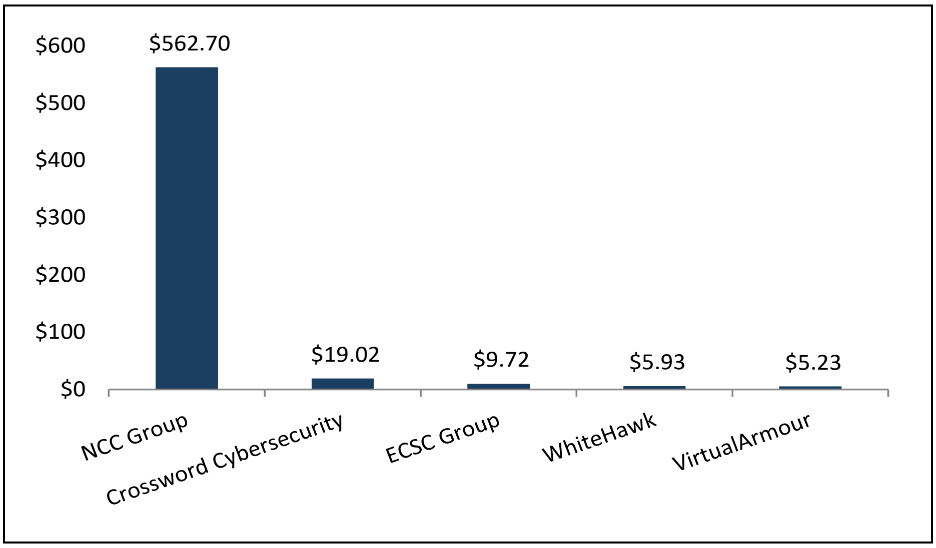
WhiteHawk operates in a blue ocean of opportunities

WHK is uniquely positioned as the first operator of a B2B e-commerce platform for cybersecurity solutions. While there are no direct competitors, some companies do come close. They operate in the B2B cyber risk assessment and profiling industry:

– RiskRecon. A Utah-based IT company, RiskRecon offers solutions for vendor security assessment to control third-party risk. The primary target markets for the company are finance, insurance, healthcare, energy and defence.

– SecurityScorecard. A New York-based IT security company, SecurityScorecard offers a SaaS platform, which provides cybersecurity ratings and continuous monitoring of third-party risk. The company also provides cloud-based solutions for assessment of security posture for various cyber threats and serves Fortune 1000 organisations globally via service and integration partners.

Figure 9: Market capitalisation for peer companies (in US$m)



Source: Pitt Street Research

RiskRecon and SecurityScorecard are private companies. The following publicly listed companies of varying size (Figure 9) provide an additional view of the WHK's competitive environment:

– NCC Group (LSE:NCC). Based in Manchester, UK, NCC is a global provider of cybersecurity and risk mitigation services. The company offers cyber security services, such as penetration testing and security assessments, to companies in transport, finance, small business and retail.

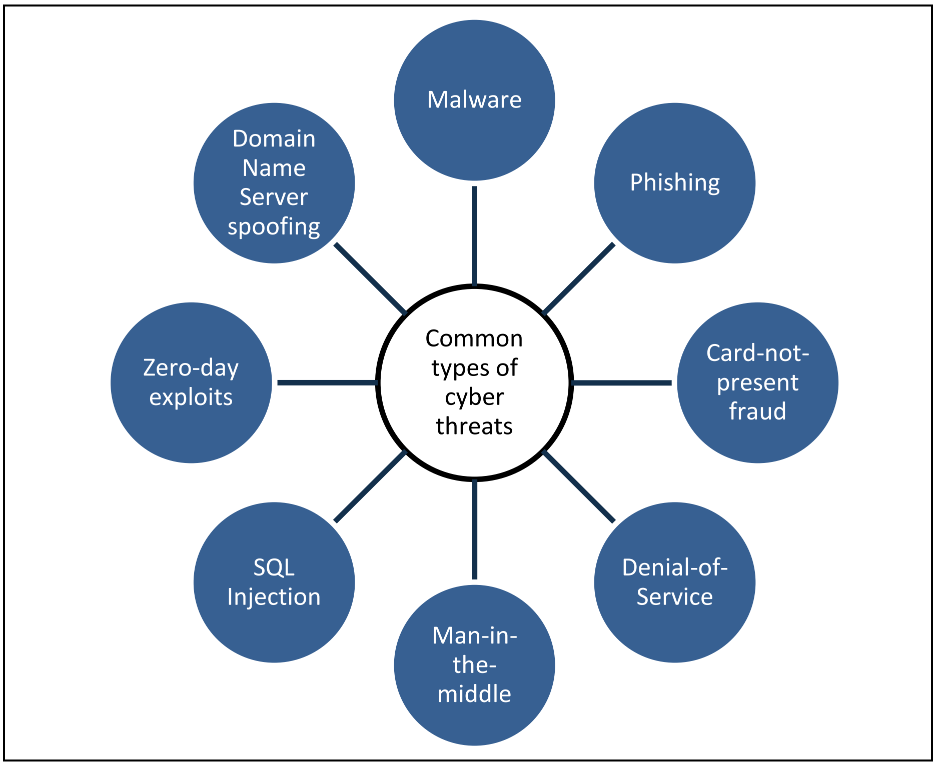
– Crossword Cybersecurity (AIM:CCS). A London-based provider of cybersecurity software and consultation services to companies in the UK and Poland. The company offers Rizikon Standard, a cyber risk and GDPR compliance assessment tool, to SMBs. Additionally, it also provides a SaaS solution, Rizikon Assurance, to large corporations to manage third-party assurance.

- ECSC Group (AIM:ECSC). Based in Bradford, UK, ECSC is a provider of information and cybersecurity services. The company offers a number of services including consultancy, testing and vendor solutions. ECSC's target sectors include education, retail, financial services and local authorities in UK.
- VirtualArmour International Inc. (CNSX:VAI). VirtualArmour is a Colorado-based IT company engaged in providing network and cybersecurity solutions to enterprises. It provides managed services, such as alerting and monitoring, as well as professional services such as consulting, assessment and implementation.

The Cybersecurity Problem

As digital connectivity continues to permeate all facets of life and businesses become more dependent on the virtual economy, threats to cybersecurity rise in tandem. As per Accenture's 2019 The Cost of Cybercrime study, the average number of security breaches experienced by organisations increased 11%, from 130 in 2017 to 145 in 2018. Moreover, with the world adjusting to the new normal of remote working due to the COVID-19 pandemic, businesses face an even greater risk of cybercrime.

Figure 10: Common cyber threats



Source: Cisco, CSO Online and Pitt Street Research

The following are some of the key cyber threats faced by businesses globally (Figure 10):

- Malware: Defined by Microsoft as 'malicious software', malware comes in a variety of forms, including backdoors, downloaders, Trojans, worms and macro viruses. The software is designed to enter a system via an email attachment or a link, which then installs dangerous software on a computer and/or network. The intent is to damage a computer or network by blocking access to components (ransomware) or to transmit critical information from the hard drive (spyware).

- Phishing: An increasingly common cyber threat, phishing involves fraudulent communication, usually sent through emails, which appears to come from a credible source. The goal is to steal sensitive information, such as credit card details and login credentials.

Card-not-present fraud is particularly hurtful to smaller businesses

- Card-not-present fraud: It is a form of credit card fraud, wherein the attacker is able to conduct transactions even without being in possession of the credit card, i.e. via online channels. The attacker obtains credit card details via hacking or phishing and uses them to carry out unauthorised transactions without having to steal the original card. The ultimate burden of these frauds is borne by businesses and their banks.

- Denial-of-service: It is a form of attack whereby the cybercriminal tries to disrupt the operations of an online service by flooding the servers or systems with traffic. Due to the sudden increase in the number of requests, the resources and bandwidth of the business get exhausted, making its services unavailable to everyone.

  Another variation of this attack is the distributed-denial-of-service attack (DDOS). Here, the attackers use multiple computers, which have already been compromised via malware, to launch the attack.

- Man-in-the-middle (MitM): MitM refers to a form of attack whereby the cybercriminal intervenes in a two-party transaction. Generally, attackers position themselves between a potential victim's device and the website or network they are trying to access. By doing this, they are able to obtain sensitive information, such as banking passwords, being shared by the user.

- SQL injection: Many websites and web forms store user information in databases designed to obey commands in SQL (structured query language). This makes them vulnerable to SQL injection attacks, wherein an attacker injects a dangerous code in the target's server. By doing this, the attacker is able to not only access sensitive user information (such as name, address and contact details), but also give the database commands in SQL to execute.

- Zero-day exploits: In case of detection of a network or software vulnerability, like in Windows, it usually takes quite some time for a patch or solution to be distributed by the provider of the software to all systems across a network. This gives attackers a window of opportunity to attack systems in the network that have not yet downloaded the security update.

- Domain name server (DNS) spoofing: It is a form of attack wherein cybercriminals use fake DNS records, which are made to resemble the original destination, in order to redirect traffic to their website. Once the target accesses the fraudulent website, the attacker is able to steal their sensitive information by prompting the target to login to their account.

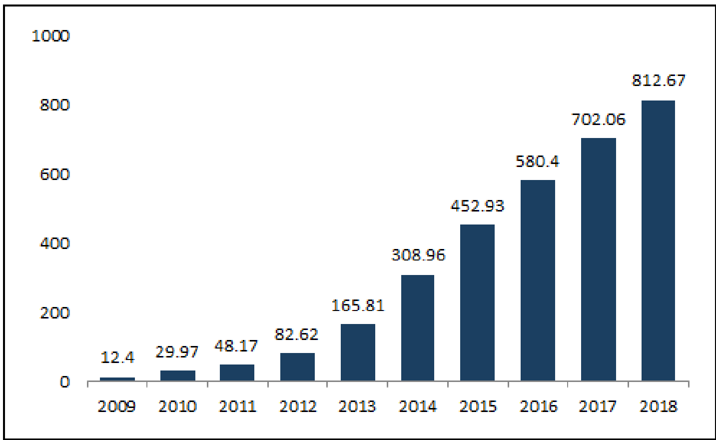
The frequency of cyber-attacks is on the rise

Digitisation of the economy facilitates rise in cyber crime

The last decade has seen a rapid increase in the number of cyber-attacks, underpinned by the digitisation of the global economy (Figure 11). As more data and sensitive information reaches servers and online databases, there is a corresponding increase in the risk of a breach.

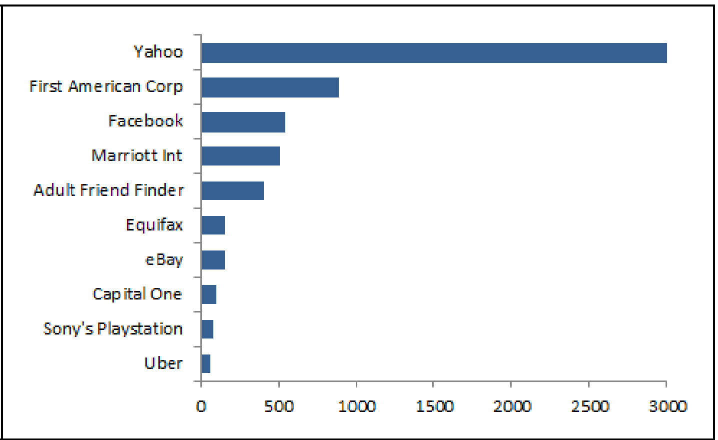
Recent history shows that when it comes to cybercrime, no business or institution is infallible. Notably, the largest data breach to-date was experienced by Yahoo (Figure 12), which in 2016 announced that all 3bn of its user accounts in 2013 were hacked by an unauthorised third party. This breach was followed by another breach in 2014, which is believed to be conducted by state-sponsored hackers, who attacked about 500m accounts.

Figure 11: Total malware infection growth rate (in millions)



Source: PurpleSec – 2019 Cyber Security Statistics

Figure 12: Some of the biggest data breaches worldwide



Source: BBC Reports

Notably, not all attacks are driven by monetary or espionage motives. Some cases, such as the 2019 Capital One breach, indicate the prevalence of freelance white-hat hacking. The stolen data, which included birthdates and social security numbers (SSNs) gathered via hundreds of thousands of credit card applications, never appeared on the dark web for sale. Nonetheless, the incident did put a dent in the company's reputation and consumers' trust in management.

Cybercriminals are expanding their web to include government organisations and smaller business – WHK's target market

While earlier attacks were focussed on big corporations and financial institutions, attackers are now casting a wider web. From government departments, such as the US Customs and Border Protection Agency, to television broadcast channels, such as the Weather Channel or TV Monde, no one is safe from cybercriminals. Increasingly, hospitals and educational institutions are also being targeted in order to obtain sensitive information, such as names, addresses and SSNs.

Moreover, cybercriminals are also moving down the food chain, attacking small and midsized businesses. As per Verizon's *2019 Data Breach Investigations Report* (DBIR), small businesses formed the largest category of victims at 43%, followed by public sector entities (16%) and healthcare organisations (15%).

The cost of cybercrime is rising fast

Not only are cyber-attacks becoming more frequent, their cost to businesses and organisations is also on the rise. As per IBM's 2019 *Cost of a Data Breach* report, the global average cost of a data breach increased 12% from US$3.5m in 2014 to US$3.92m in 2019.

Notably, among the regions assessed by the report, the US continues to register the most expensive data breaches. The average total cost of a data breach experienced by a US-based company stood at US$8.19m in 2019, which is more than double the global average.

Damage from cybercrime is higher for smaller businesses

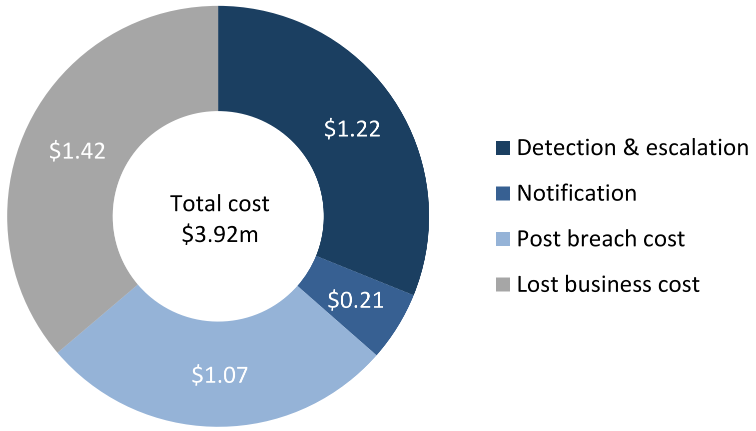
Data breach cost is higher for SMBs as compared to larger organisations

A data breach is particularly hurtful to smaller businesses, underpinned by lack of economies of scale. As per the IBM report, the total cost for large organisations (more than 25k employees) averaged at US$204 per employee. On the other hand, the average cost of a data breach stood at a colossal US$3,500 per employee for smaller companies (500 to 1000 employees).

Due to lack of sophisticated cybersecurity tools and an active cybersecurity strategy, SMBs often experience a delay in detection of a breach, leading to aggravation of the situation. Add to this the significant costs of mandatory forensic examination, notification to customers, compliance fines, system upgrades etc., and the bill can reach a whopping average of US$2.65m for smaller companies. This severely impacts the bottom line and can even push smaller businesses into bankruptcy.

In addition to direct costs, data breaches also tarnish business reputations. This leads to loss of business, which has a long-term impact on the company. Notably, as per the IBM report, loss of business forms the biggest chunk of the total breach cost, accounting for 36.2% (Figure 13).

Figure 13: Breakdown of data breach cost (in $m)



Source: IBM Security – Cost of a data breach report (2019)

Breaches caused by third parties, e.g. suppliers, amplify the costs of cyber crime

Additionally, third-party breaches are particularly painful for businesses. As per IBM, in cases of data breach caused by a third party, such as a vendor or supplier, the cost increased by more than US$370,000, to reach an average total cost of $4.29m.

With WHK offering in-depth risk assessment profiling and analysis of vendor companies, we believe it is well-positioned to see significant growth in this vertical.

Valuation

Using a blended valuation approach (DCF, EV/Sales), we value WHK at A$0.35 per share base case and A$0.41 per share bullish case.

Revenue Drivers

We modelled WHK's operating revenues by analysing each of its key product lines and respective customers. Our methodologies are as follows:

Cyber Risk Radar

In the Cyber Risk Radar segment, which runs on a recurring SaaS revenue model, our forward revenues are driven by the estimated number of new Government and Enterprise contract wins and the expected annualised contract revenue (ACR).

Attractive pricing position for Cyber Risk Radar product line

Based on the product pricing range guided by the company, our base case assumed an ACR of US$500K, whilst our bullish case increased ACR to US$600K. In terms of near-term contract wins, our base case assumes WHK can secure five new contracts for FY20 as the firm is currently advancing several Cyber Risk Radar proposals with customers.

Additionally, by leveraging the new CMMC policies, WHK should be able to lock in further Cyber Risk Radar contracts with Enterprise and Government customers over the short to medium term, in our view.

Cyber Risk Program

For the Cyber Risk Program segment, which also runs on a recurring SaaS revenue model, we applied similar methodology in forecasting its sales.

Surge in sales expected due to a rise in COVID-19 related cybercrime

Our ACR is estimated at US$100K base case and US$120K bullish case. With US$400K in annual SaaS revenue already achieved thus far in FY20, we expect revenue to ramp up to US$1.2M by FY20 year-end as WHK expands its marketing and tendering activity going forward.

Within our estimated US$1.2M FY20 revenue, it is worth noting that WHK is expected to retain only a certain portion of the total amount, which we have assumed to be a conservative, due to its revenue sharing partnership with an unnamed global consulting firm.

Digital Age Business Risk Suite

Potential sales of SME Business Suite to tens of thousands of SMB customers

In the SME Business Risk Suite segment, we expect initial sales to occur in FY21 as WHK has now integrated its cyber risk solution into Sontiq's SME Suite. By leveraging Sontiq's established customer base, we expect WHK to rapidly build up its SMB revenue stream through the sale of its integrated cybercrime software to potentially tens of thousands of SME customers.

Our revenue model for this segment is driven by the composition of WHK's cyber risk bundle solutions (Basic, Balanced & Advanced) and the respective annualised recurring revenue for each bundle per SME customer.

Our base case assumes half of SME customers will purchase WHK's Basic bundle solution, whilst our bullish case is comparatively skewed towards WHK's Balanced and Advanced bundle solutions.

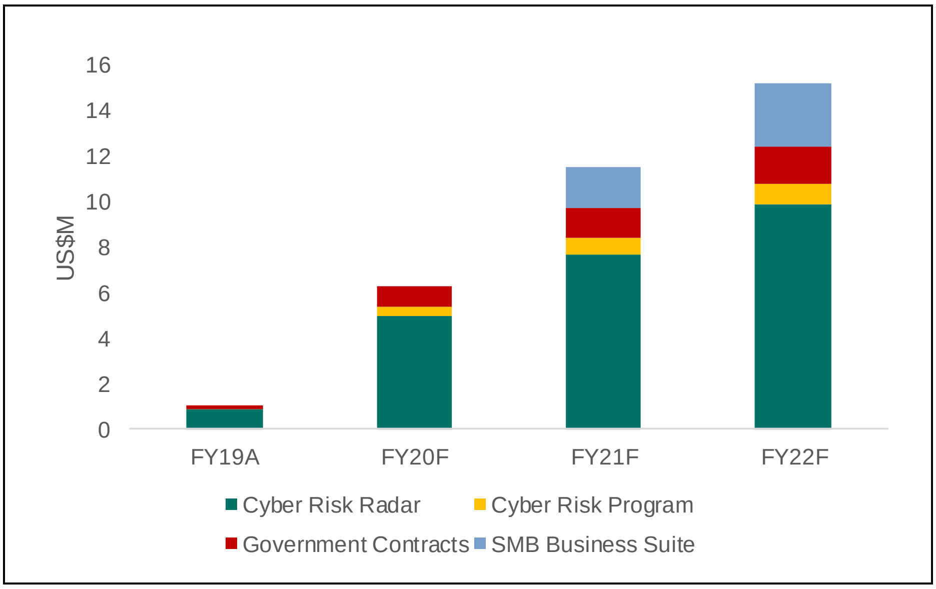
As discussed earlier, pricings also vary among each bundle type. We applied the lower end of WHK's pricing range for our base case, whilst our bullish case attracted a slight premium in pricing.

We may see larger revenue contributions come in if and when WHK is able to sign wholesale agreements for its SME Digital Age Business Risk Suite with financial institutions and MSP's.

We then derive WHK's revenue share by accounting for its sales commission (10% base case, 15% bullish case) as well as Sontiq's 15% revenue share.

Figure 14 shows our base case segment revenue model from FY20 to FY22.

Figure 14: WhiteHawk's operating revenue, actual and forecast



Source: Company Report, Pitt Street Research

Based on our base case assumptions, we forecast a significant rise in WHK's operating revenues for FY20, with the greatest contribution coming from Cyber Risk Radar, largely due to its premium pricing position. It is also worth noting that we expect to see WHK generating more revenues from Cyber Risk Program.

We project that the SME Business Suite revenues will commence in FY21 as the business launches an integrated cyber risk offering to SME customers. Over the FY19 to FY22 period, we estimated revenue CAGR of 145% per annum. Figure 15 shows our revenue bridge between FY19 actual revenue and our FY20 estimated revenue.

Enhanced margins through greater scale and efficiency

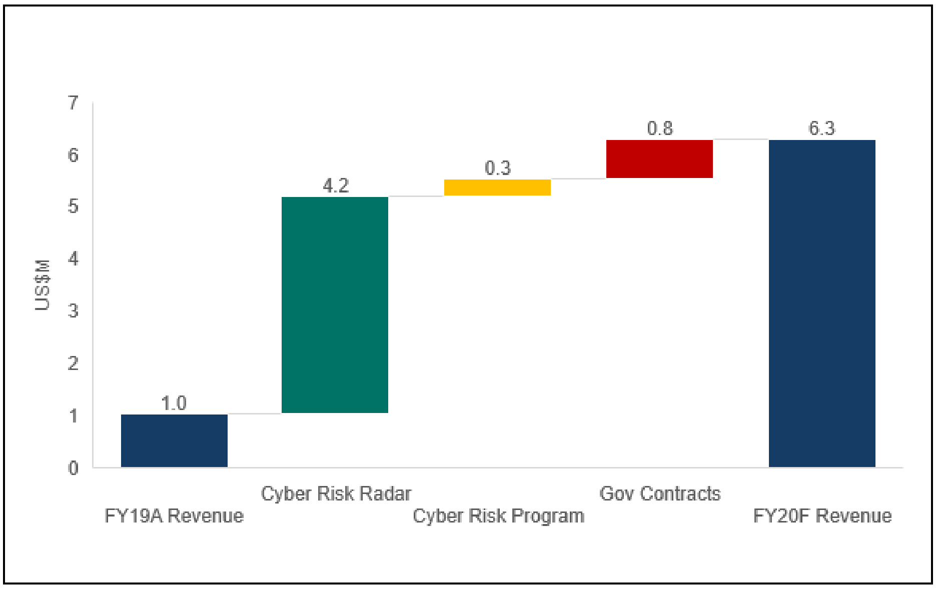
We note that WHK's gross margin in FY19 has improved to 49% as a result of the firm's investments in automation. To be conservative, we assume that WHK's FY20 gross margin remains at the same 49% level as reported in FY19. In the medium term, as the company achieves greater scale and efficiency, we assume that its gross margins will gradually improve to 53% by FY22.

EBITDA and NPAT break even by FY22

Moreover, by continuing to ensure performance and delivery efficiency, WHK's operating margins should also improve post breakeven, in our view. We expect the company to break even at the EBITDA and NPAT levels in FY22.

On fixed operating costs, we assumed an annual increase of 2.75% on rental cost as per the lease agreement. On staff cost, we factored in wage inflation.

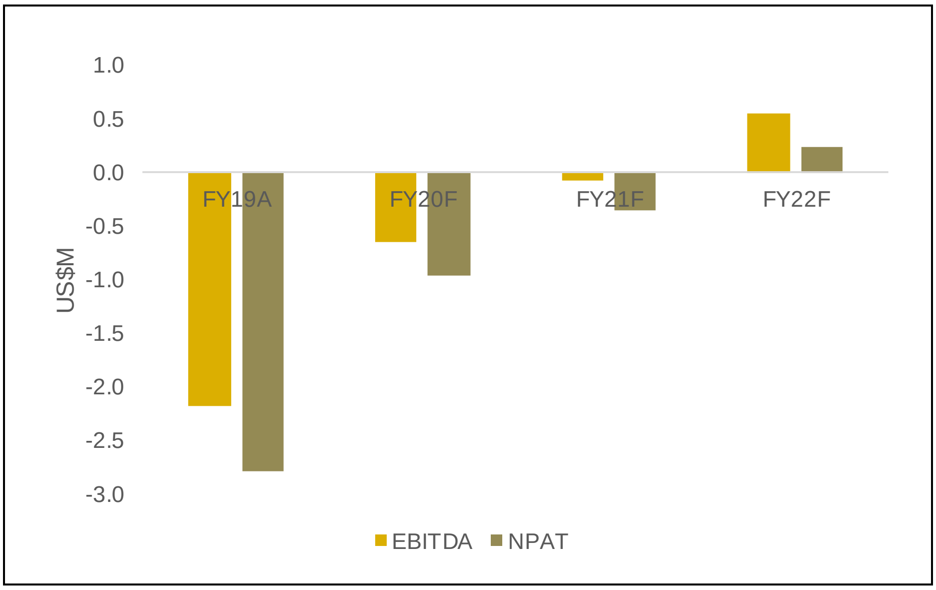
Figure 15: Revenue bridge between FY19A and FY20F



Source: Company Report, Pitt Street Research

Based on our base case modelling, we expect WHK's net loss for FY19 to improve by US$1.8M to a net loss of US$1.0M by FY20. Overall, we expect WHK to achieve bottom-line profitability by FY22 (Figure 16).

Figure 16: WhiteHawk's EBITDA and NPAT, actual and forecasts



Source: Company Report, Pitt Street Research

Discounted Cash Flow value range of A$0.47-0.58 per share

A conservative discount rate of 12% has been applied in valuing WHK

Our key Discounted Cashflow modelling assumptions are as follows:

- Our DCF model is predominantly driven by forward revenues coming from WHK's major product lines, being Cyber Risk Radar, Cyber Risk Program and SMB Business Suite. These forward revenues are dependent on WHK's ability to win new Government, Enterprise and SMB customer contracts as well as its ability to retain existing customers. Refer to Revenue Drivers on the next page for more detail.
- **Forecast Horizon.** We applied an 11-year forecast horizon as WHK is in its initial revenue ramp up phase and is experiencing high revenue growth. This is followed by a terminal growth rate of 2%.
- **Discount Rate.** We assumed a discount rate of 12% as the company is still in the early stages of its life cycle. Additionally, its sales cycles may be long and unpredictable, which can result in lumpy cash flows over the short to medium term. We believe the equity risk premium should be elevated to account for firm-specific risks including potential delays in the implementation of customer contracts. As the company achieves greater scale with recurring revenues becoming more dominant, we will look to reduce our discount rate accordingly.
- **Funding.** We assumed that WHK will successfully secure A$1.5M in equity funding from RiverFort Global Opportunities. Post FY20, we expect the company to self-fund its operations through its internal cash flows.
- **Corporate Tax.** We assumed a corporate tax rate of 27%. As WHK has a significant amount of tax losses to carry forward, our base case modelling expects the company to pay its first cash tax in FY25.
- **Exchange rate.** 0.64 USD/AUD is assumed.

Figure 17 shows our DCF valuation summary for WHK.

Figure 17: DCF Valuation Summary

Base Case Valuation	
Present value of FCF (m)	16.2
Present value of Terminal FCF	38.2
Enterprise Value (m)	**54.4**
Net debt (cash) (m)	(1.3)
Minority interest (m)	0.0
Equity value (m)	55.7
Share outstanding (Diluted)	186.6
Implied price (USD)	0.30
USD/AUD	0.64
Implied price (AUD)	0.47
Current price (AUD)	0.051
Upside (%)	814%

Bull Case Valuation	
Present value of FCF (m)	21.7
Present value of Terminal FCF	46.3
Enterprise Value (m)	**68.0**
Net debt (cash) (m)	(1.3)
Minority interest (m)	0.0
Equity value (m)	69.3
Share outstanding (Diluted)	186.6
Implied price (USD)	0.37
USD/AUD	0.64
Implied price (AUD)	0.58
Current price (AUD)	0.051
Upside (%)	1038%

Source: Pitt Street Research

Relative Valuation: A$0.22 per share

Peer group analysis of cybersecurity and SaaS players

We have included a blend of seven ASX-listed companies and three NASDAQ-listed companies in our peer group analysis for WHK (Figure 18), of which six are active in cyber security while others operate a SaaS subscription model similar to WHK's.

Figure 18: WHK's peer group analysis

Company Name	Ticker	Reporting Year	Operating Regions	Market Cap (A$M)	FY20 EV / Sales
Cybersecurity Companies					
ArchTIS	ASX:AR9	Jun-20	US, Europe, ANZ	9.2	6.2x
Vault Intelligence	ASX:VLT	Jun-20	ANZ, China	24.3	3.1x
Tesserent	ASX:TNT	Jun-20	Australia	29.2	0.9x
SecureWorks Corp	NASDAQ:SCWX	Jan-21	Global	1,434.0	1.4x
Check Point Software Technologies	NASDAQ:CHKP	Dec-20	Global	23,945.1	6.8x
Fortinet	NASDAQ: FTNT	Dec-20	Global	27,989.8	6.4x
Other ASX SaaS providers					
MSL Solutions Limited	ASX:MPW	Jun-20	Europe, US, Middle East	11.9	0.5x
Damstra Holdings Limited	ASX:DTC	Jun-20	ANZ, North America, Europe	125.5	5.7x
Class Limited	ASX:CL1	Jun-20	Australia	169.4	3.5x
Whispir	ASX:WSP	Jun-20	US, APAC	190.4	4.6x
Average					**3.9x**
Median					**4.0x**
WhiteHawk Limited	**ASX:WHK**	**Dec-20**	**US**	**8.1**	**0.7x**

Source: Company Report, Pitt Street Research

As illustrated, WHK is currently trading at a significant discount to the peer group median of 4.0x FY20 revenue. We think WHK's undervaluation relative to its peer group is due to investors unawareness of WHK, as well as their lack of familiarity with cybersecurity generally.

We believe WHK is on a solid commercialisation path based on the strong pipeline of contract opportunities across the US industries. Should WHK be able to execute according to its plan, we think its trading multiple will likely re-rate towards its peer group median.

If revenue can rise to US$6.3M in FY20 as per our base case forecast and assuming an EV/Sales multiple equivalent to the peer group median of 4.0x, that would imply an enterprise value of US$25.4M, which adjusted for US$1.3M of net cash points to an equity value of US$26.7M.

Applying a diluted share base of 186.6M and factoring in an exchange rate of 0.64 USD/AUD, we arrive a value of A$0.22 per WHK share (Figure 19).

Figure 19: EV/Sales Multiple Valuation Summary

Equity value determination (AUDm unless specified otherwise)	EV / Sales
EV/Sales Multiple	4.0
Discount/ Premium	0.0%
Sales FY20e	6.3
Implied EV	25.4
Net debt (cash)	(1.3)
Minority interest	-
Equity/Book value	**26.7**
Diluted Shares	186.6
Implied price (AUD)	**0.22**
Current price (AUD)	0.051
Upside (%)	*339%*

Source: Pitt Street Research

Blended valuation range of A$0.35-0.41 per share

Our blended valuation, equally weighted between DCF and EV/Sales, yields a value of A$0.35 per share base case and A$0.41 per share in a bullish scenario (Figure 20).

Figure 20: Blended Valuation Summary

Base Case	Weights (%)	Share price (AUD)
DCF	50.0%	0.47
Relative valuation	50.0%	0.22
Composite Value (AUD)		**0.35**
Current Price (AUD)		0.051
Upside/ Downside (%)		**576.5%**

Bull Case	Weights (%)	Share price (AUD)
DCF	50.0%	0.58
Relative valuation	50.0%	0.25
Composite Value (AUD)		**0.41**
Current Price (AUD)		0.051
Upside/ Downside (%)		**709.4%**

Source: Pitt Street Research

Conclusion

Through WHK's proprietary technology to assess, identify and provide options to mitigate cyber threats, the company has opened up a large addressable market in the Government and Enterprise verticals through subcontracting with larger business partners. At the same time, it is able to address the SME market for cyber security through its partnership with Sontiq.

Combined with its revenue sharing agreements with many cyber security solutions providers that can sell through Cyber Risk Marketplace, we believe WHK has developed an attractive and highly scalable business model.

We value the company at A$0.35 per share.

Appendix I: Senior Management and Board of Directors

	Name and Designation	Profile
	Terry Roberts **Chief Executive Officer & Founder**	Prior to WhiteHawk, Terry Roberts was the TASC Vice President for Cyber Engineering and Analytics, running all Cyber/IT, Financial and Business Analytics cross cutting, innovative technical services. Prior to that, she was the Executive Director of the Carnegie Mellon, Software Engineering Institute, leading the technical body of work for the entire US Interagency with a special focus on leveraging and transitioning commercial innovation and acquisition excellence to government programs and capabilities and establishing the Emerging Technologies Center and Cyber Intelligence Consortium. Before transitioning to industry in 2009, Terry Roberts was the Deputy Director of Naval Intelligence (DDNI), where she led more than 20,000 intelligence and information-warfare military and civilian professionals together with the Director of Naval Intelligence. She managed more than $5 billion in resources, technologies and programs globally. She helped lead the initial approach for the merging of Naval Communications and Intelligence under the OPNAV N2/N6 and the creation of the Information Dominance Corps. Prior to being the Navy DDNI, Terry Roberts served as the Director of Requirements and Resources for the Office of the Under Secretary of Defence for Intelligence (USDI), spearheading the creation and implementation of the Military Intelligence Program (MIP), in partnership with the Director of National Intelligence, the Services, the Combat Support Agencies and the Office of the Secretary of defence (OSD).
	Soo Kim **Chief Product Officer**	Soo Kim is WhiteHawk's Chief Product Officer (CPO). In this role, she is responsible for WhiteHawk product and service vision, strategy, design, development, and delivery. She is also responsible for ensuring the ecosystem is continuously improved to deliver an easy, intuitive, and enabling set of online customer services and offerings. Prior to joining WhiteHawk, Soo worked as the Cybersecurity, Technology Strategy expert at Accenture Federal Services. She has also been a Business Consultant Architect at Hewlett Packard Enterprise Services, Vice President and Technology Director at TASC, and a Software Development Engineer at numerous commercial and federal contractor companies. Across these roles, Soo has provided leadership for the development of cybersecurity assets and capabilities in support of clients; served as the technical lead on multiple prime bids; and established and integrated best practices for business operations and continuity, customer program execution, business growth, and financial management and reporting. Soo brings experience in providing technical and business leadership with a focus on strategic planning, tactical execution, business operations, and solutions delivery. She has her bachelor's degree in Mathematics from Virginia Tech and is a Certified Enterprise Architect and Scrum Master.

	Kevin Goodale **Chief Financial Officer**	Kevin Goodale is a co-founder of WhiteHawk and is currently Chief Financial Officer (CFO). In this role, Kevin is responsible for the administration of WhiteHawk to include the accounting and human resources functions. As CFO, Kevin is responsible for the complete accounting cycle, banking and finance relationships, payroll management, accounts receivable and accounts payable management. Prior to WhiteHawk, Mr. Goodale served as the CFO for Impressions Marketing Group Inc. He is a career commercial financial and contracting manager with over 20 years of experience at the CFO level. His experience ranges across retail, construction and manufacturing businesses with revenues of US$12M to US$80M and multiple locations.
	Philips George **Non-Executive Director**	Philips George has experience as a manging director and CEO with a strong background in Fintech, cyber security and IT networking. He has previously worked as a CEO, CTO, general manager and Operations Manager. For the last eleven years Mr. George primarily serviced the Finance, Oil & Gas, Start-up & Mining and Petrochemical industries. He is also the former operations manager of Uber Australia.
	Louise McElvogue **Non-Executive Director**	Louise McElvogue is a non-executive director experienced in building digital businesses, leading innovation and managing risk for boards, corporates and start-ups globally. She is an industry professor, Data and Digital, at UTS Business School and a fellow of the Australian Institute of Company Directors. She has led more than 30 digital products in the US, Europe and Australia, working on Consumer Digital applications, business change and growth strategies for companies including McDonalds, British Gas, Newscorp and the BBC.
	Tiffany Kleemann **Non-Executive Director**	Tiffany Kleemann is currently the SVP of Imperva. She joined Imperva in July 2019 through the acquisition of Distil Networks where she was CEO. She was formerly VP of Global Strategic Partnerships and Alliance Operations at FireEye, SVP of Client Solutions and Chief Revenue Officer for iSight and Mandiant as well as former Deputy Chief of Staff at the White House Office of Cyber Security and Critical Infrastructure Protection and a decorated US Coast Guard officer.

Appendix II: Risks

We have identified three key risks associated with WHK's investment thesis:

1. Execution risk: Even though WHK already has several products in the market, the company will still need to demonstrate it can successfully roll out its current and future products across a diversified customer base, ultimately reflected in long term revenue growth.
2. Funding risk: WHK may need additional funding to execute its strategy going forward. As recent market events have shown, financial markets are unpredictable and may not always be accessible by WHK. Additionally, as a small cap company, WHK may not always be in a good position to get the best terms to raise capital.
3. Reputational risk: Even though WHK doesn't claim to be able to provide 100% security from cybercrime, a potential cybersecurity breach at one of its customers could potentially have adverse effects on its reputation as a cybersecurity company in the market.

Appendix III: Analyst certification

Marc Kennis, lead analyst on this report, has been covering a range of different sectors as an analyst since 1997.

- Marc obtained an MSc. in Economics from Tilburg University, The Netherlands, in 1996 and a Post Grad. in investment analysis in 2001.
- Since 1996, he has worked for a variety of brokers and banks in The Netherlands, including ING and Rabobank, where his main focus has been on the Technology sector, including the Semiconductor sector.
- After moving to Sydney in 2014, he worked for several Sydney-based brokers before setting up TMT Analytics Pty Ltd, an issuer-sponsored equities research firm.
- In July 2016, with Stuart Roberts, Marc co-founded Pitt Street Research Pty Ltd, which provides issuer-sponsored research on ASX-listed companies across the entire market, including Technology companies.

Cheng Ge is an equities research analyst at Pitt Street Research.

- Cheng obtained a B.Com in Finance and LL.B from University of New South Wales, in 2013, and has passed all three levels of the CFA Program.
- Prior to joining Pitt Street Research, he has worked for several financial services firms in Sydney, where his focus was on financial advice.
- He joined Pitt Street Research in January 2020.

WhiteHawk Limited

Profit & Loss (USD m)	2017a	2018a	2019a	2020e	2021e	2022e	2023e	2024e
Sales Revenue	**0.1**	**0.5**	**1.0**	**6.3**	**11.5**	**15.2**	**19.2**	**22.9**
Operating expenses	(2.6)	(3.6)	(3.2)	(6.9)	(11.6)	(14.7)	(17.8)	(20.4)
EBITDA	**(2.5)**	**(3.1)**	**(2.2)**	**(0.7)**	**(0.1)**	**0.6**	**1.4**	**2.5**
Depn & Amort	(0.0)	(0.4)	(0.6)	(0.3)	(0.3)	(0.3)	(0.4)	(0.5)
EBIT	**(2.5)**	**(3.5)**	**(2.8)**	**(1.0)**	**(0.3)**	**0.2**	**1.0**	**2.0**
Net Interest	(0.3)	(0.0)	(0.0)	(0.0)	(0.0)	(0.0)	(0.0)	(0.0)
Profit before tax	**(2.8)**	**(3.5)**	**(2.8)**	**(1.0)**	**(0.3)**	**0.2**	**1.0**	**2.0**
Tax expense	-	-	-	-	-	-	-	-
NPAT	**(2.8)**	**(3.5)**	**(2.8)**	**(1.0)**	**(0.3)**	**0.2**	**1.0**	**2.0**

Cash Flow (USD m)	2017a	2018a	2019a	2020e	2021e	2022e	2023e	2024e
Profit after tax	(2.8)	(3.5)	(2.8)	(1.0)	(0.3)	0.2	1.0	2.0
Depreciation	0.0	0.4	0.6	0.3	0.3	0.3	0.4	0.5
Change in trade and other receivables	0.1	(0.1)	(0.2)	(1.5)	(1.0)	(0.4)	(0.5)	(0.4)
Change in trade payables	0.0	0.0	0.1	1.1	0.5	0.0	0.0	(0.0)
Other operating activities	1.6	0.7	0.5	0.4	0.7	1.0	1.2	1.4
Operating cashflow	**(1.1)**	**(2.5)**	**(1.8)**	**(0.7)**	**0.2**	**1.1**	**2.1**	**3.5**
Capex (- asset sales)	(1.3)	(0.5)	(0.0)	(0.3)	(0.5)	(0.6)	(0.8)	(0.9)
Other investing activities	(0.0)	-	-	-	-	-	-	-
Investing cashflow	**(1.4)**	**(0.5)**	**(0.0)**	**(0.3)**	**(0.5)**	**(0.6)**	**(0.8)**	**(0.9)**
Dividends	-	1.0	2.0	3.0	4.0	5.0	6.0	7.0
Equity raised	3.4	1.1	2.6	1.0	-	-	-	-
Debt drawdown (repaid)	-	-	(0.3)	0.3	(0.3)	-	-	-
Other financing activities	5.3	(1.2)	(1.0)	(2.3)	(4.1)	(5.0)	(6.0)	(7.0)
Financing cashflow	**8.6**	**0.9**	**3.4**	**1.9**	**(0.4)**	**-**	**-**	**-**
Net change in cash	**6.2**	**(2.0)**	**1.5**	**1.0**	**(0.7)**	**0.5**	**1.4**	**2.6**
Cash at End Period	3.7	1.3	1.6	1.8	1.3	1.8	3.1	5.7
Net Debt (Cash)	(3.7)	(1.3)	(1.3)	(1.4)	(1.1)	(1.6)	(2.9)	(5.5)

Balance Sheet (USD m)	2017a	2018a	2019a	2020e	2021e	2022e	2023e	2024e
Cash	3.7	1.3	1.5	1.8	1.3	1.8	3.1	5.7
Total Assets	5.1	2.9	3.0	4.8	5.4	6.6	8.8	12.2
Total Debt	-	-	0.2	0.5	0.2	0.2	0.2	0.2
Total Liabilities	1.0	0.8	0.7	2.1	2.3	2.3	2.4	2.3
Shareholders' Funds	4.1	2.1	2.3	2.7	3.1	4.3	6.4	9.9

Ratios	2017a	2018a	2019a	2020e	2021e	2022e	2023e	2024e
Net Debt/Equity (%)	-90.0%	-62.0%	-57.5%	-51.1%	-34.7%	-36.4%	-45.2%	-55.8%
Return on Equity (%)	nm	nm	nm	nm	nm	5.4%	15.0%	20.4%

General advice warning, Disclaimer & Disclosures

Terms & Conditions

The information contained herein ("Content") has been prepared and issued by Pitt Street Research Pty Ltd ACN 626365615 ("Pitt Street Research"), an Authorised Representative (no: 1265112) of BR Securities Australia Pty Ltd. ABN 92 168 734 530, AFSL 456663. All intellectual property relating to the Content vests with Pitt Street Research unless otherwise noted.

Disclaimer

Pitt Street Research provides this financial advice as an honest and reasonable opinion held at a point in time about an investment's risk profile and merit and the information is provided by the Pitt Street Research in good faith. The views of the adviser(s) do not necessarily reflect the views of the AFS Licensee. Pitt Street Research has no obligation to update the opinion unless Pitt Street Research is currently contracted to provide such an updated opinion. Pitt Street Research does not warrant the accuracy of any information it sources from others. All statements as to future matters are not guaranteed to be accurate and any statements as to past performance do not represent future performance.

Assessment of risk can be subjective. Portfolios of equity investments need to be well diversified and the risk appropriate for the investor. Equity investments in a listed or unlisted company yet to achieve a profit or with an equity value less than $50 million should collectively be a small component of an individual investor's equity portfolio, with smaller individual investment sizes than otherwise. Investors are responsible for their own investment decisions, unless a contract stipulates otherwise.

Pitt Street Research does not stand behind the capital value or performance of any investment. Subject to any terms implied by law and which cannot be excluded, Pitt Street Research shall not be liable for any errors, omissions, defects or misrepresentations in the information (including by reasons of negligence, negligent misstatement or otherwise) or for any loss or damage (whether direct or indirect) suffered by persons who use or rely on the information. If any law prohibits the exclusion of such liability, Pitt Street Research limits its liability to the re-supply of the Information, provided that such limitation is permitted by law and is fair and reasonable.

General Advice Warning

The Content has been prepared for general information purposes only and is not (and cannot be construed or relied upon as) personal advice nor as an offer to buy/sell/subscribe to any of the financial products mentioned herein. No investment objectives, financial circumstances or needs of any individual have been taken into consideration in the preparation of the Content.

Financial products are complex, entail risk of loss, may rise and fall, and are impacted by a range of market and economic factors, and you should always obtain professional advice to ensure trading or investing in such products is suitable for your circumstances; ensure you obtain, read and understand any applicable offer document.

Disclosures

Pitt Street Research has been commissioned to prepare the Content. From time to time, Pitt Street Research representatives or associates may hold interests, transact or hold directorships in, or perform paid services for, companies mentioned herein. Pitt Street Research and its associates, officers, directors and employees, may, from time to time hold securities in the companies referred to herein and may trade in those securities as principal, and in a manner which may be contrary to recommendations mentioned in this document.

Pitt Street Research receives fees from the company referred to in this document, for research services and other financial services or advice we may provide to that company. The analyst has received assistance from the company in preparing this document. The company has provided the analyst with communication with senior management and information on the company and industry. As part of due diligence, the analyst has independently and critically reviewed the assistance and information provided by the company to form the opinions expressed in the report. Diligent care has been taken by the analyst to maintain an honest and fair objectivity in writing this report and making the recommendation. Where Pitt Street Research has been commissioned to prepare Content and receives fees for its preparation, please note that NO part of the fee, compensation or employee remuneration paid will either directly or indirectly impact the Content provided.