For personal use only

FOR IMMEDIATE RELEASE
14 September 2018

WhiteHawk 360 Cyber Risk Framework Contract Pipeline
For Real-Time Vendor Cyber Risk Management

Highlights

- **Tailored versions of the 360 Cyber Risk Framework provides BitSight cyber risk ratings, continuous monitoring, cyber risk alerts and WhiteHawk risk analytics, AI Risk Profile, and matching to vendor options in real-time to customers to provide continuous Insight across hundreds of vendors at once.**
- **Recent U.S. Government focus on the systemic risks posed by their IT and software supply chain vendors has been growing both at US Department of Defense and US Department of Homeland Security where Whitehawk has an existing contract.**
- **Customers in our Pipeline of potential contracts in various stages of negotiation are seeking a focus on supply chain risk analytics which is an increasing risk area as cyber attackers focus on the weakest links in a supply chain.**
- **British Airways recently reported large breach affecting over 380,000 customers may have originated through a supply chain company.**

Perth, WA and Alexandria, VA – WhiteHawk Limited (ASX:WHK) ("WhiteHawk or "the Company"), the first global online cyber security exchange enabling small-to-medium businesses to take smart action against cyber-crime and fraud, is pleased to announce a strong pipeline of contract opprtunities in the US for our 360 Cyber Risk Framework Review, including US Government. These customers are seeking to ensure protection from cybercrime that may use supply chain companies as an access pathway.

The Company currently has existing contracts with the US Government and Major Financial Institution, and is building on those existing engagements with further 360 Cyber Risk Framework Review Proof of Value contracts.

WhiteHawk is able to tailor the 360 Cyber Risk Framework to provide:

(a) Cyber risk ratings;
(b) Continuous monitoring;
(c) Cyber risk alerts and WhiteHawk risk analytics;
(d) Risk Scorecards
(e) AI risk profiling; and
(f) vendor risk mitigation matching,

WhiteHawk Cyber Risk Frameworks all provide these insights and services in real time to customers, ensuring that their supply chain companies have foundational cyber security products and services in place that can prevent and mitigate cybercrime and fraud events which result from one of their supply chain companies.

Level 28 140 St George Tce Perth WA 6000
Tel : +61 8 6311 4636, Fax : +61 8 6311 4661
ABN: 97 620 459 823
www.whitehawk.com

For personal use only

Such a supply chain cyber breach occurred on the 6th of September. British Airways reported a major breach of all customer personal and financial data inputted on their transactional website from 21 August to 5 September 2018, affecting over 382,000 customers credit and debit card details. As a result, British Airways could be fined up to One Billion Euros under the newly implemented European Commission regulations where penalties for data breaches can be levied up to 4% of the companies turnover. In addition, there is always the potential impact to company reputation and customer relations as was seen with the Target breach of 2015.

Whilst British Airways has not confirmed the attack pathway, several cyber experts have stated that this may be an example of supply chain risk. In the September 7th BBC article entitled **British Airways breach: How did hackers get in?"** "Prof Woodward of the Univeristy of Surrey points out that this is an increasing problem for websites that embed code from third-party suppliers - it's known as a supply chain attack. Third parties may supply code to run payment authorisation, present ads or allow users to log into external services." It is the vetting of such software vendors and service providers, that the WhiteHawk 360 Risk Framework is designed to Identify, address and mitigate, in advance of a breach.

WhiteHawk continues to promote tailored versions of the 360 Cyber Risk Framework to US based Financial Institutions, Manufacturers (commercial & federal), U.S. Utilities and Government and has a current pipeline of potential contracts at varying stages of negotiation to supply the 360 Cyber Risk Review and Mitigation automated approach. And has created Proof of Value initial offerings, across 40 supply chain companies, that are being implemented today.

This has positioned the company to potentially close an additional five sales of the 360 Cyber Risk Framework in 2018 and first quarter 2019 from the current pipeline. The latest customer channel focus is on the 3,200+ power and water utilities across the United States (regional power associations, regulators, and larger private utilities) who are all searching for how to gain continuous insight into and to address their cyber related risks.

Importantly, this process drives companies that are in a customer's supply chain to WhiteHawk's CyberSecurity Exchange, to mitigate key cyber risks in real-time. Some of the current pipeline companies have supply chains exceeding 500 companies.

Terry Roberts, Executive Chair of WhiteHawk, commented, "We continue to demonstrate that our Cyber Risk Frameworks are equally of impact and value across Sectors. And now we are having these conversations and demonstrations with not only financial institutions and industrial customers but also key US Government Departments (Dept of Defense, Department of Homeland Security, the Intelligence Community) and Government Owned Utilities, who are highly targeted and in great need of an effective, affordable and scalable cyber risk framework"

Terry Roberts added "Traditionally Supply Chain Company or Vendor Risk Management programs are focused primarily on financial and product/service risk checks by a large staff of personnel and business processes. WhiteHawk saw an opportunity for an end to end approach that leverages best of breed open data sets and premier risk tradecraft, baked into AI driven algorithms and analytics – all displayed in an integrated dashboard. This way WhiteHawk's risk insights can be scaled across

For personal use only

hundreds and even thousands of vendors and supply chain companies. In addition, we have integrated our WhiteHawk Cybersecurity Exchanges' ability to mitigate all critical cyber related risks."

-ENDS-

For more information:

WhiteHawk media inquiries (USA)
LeighAnne Baxter
publicrelations@whitehawk.com
+1 833 942-9237

WhiteHawk investor inquiries
(AUS)
Kevin Kye
investors@whitehawk.com

About WhiteHawk

Launched in 2016, WhiteHawk began as a cyber security advisory service with a vision to develop the first self-service cyber security exchange simplifying how businesses discover, decide, and purchase cyber security solutions. Today, we help US and Australian companies to connect to content, solutions, and service providers through evolving our rich data and user experience. WhiteHawk is a cloud-based cyber security exchange platform that delivers 'solutions on demand' for small to midsize enterprises. The platform enables customers to leverage their custom Security Story to find cyber tools, content, and relevant services through our algorithms to better understand how to improve and stay ahead of threats. The Platform enables companies to fill their needs on an ongoing basis with demonstrated cost and time savings. For more information, visit www.whitehawk.com.