WHITEHAWK

Cyber Risk Scorecard

On Company: Sample

Prepared for:

Sample Use

Prepared by:

Andres Ramos

Cyber Analyst

andres.ramos@whitehawk.com

Prepared on:

January 18, 2021

Table of Contents

WhiteHawk Cyber Risk Scorecard

WhiteHawk's Cyber Risk Scorecard provides businesses and organizations a topline cyber risk snapshot as an indicator of a company's effectiveness at addressing the impacts of online crime and fraud. We use a risk rating ranging from 250 to 900 based upon over 23 cyber risk controls. Our Cyber Analysts provide context and analytics that augment the risk indicators obtained through our partner, BitSight Technologies, enabling companies to take action to mitigate cyber risks to their revenue, reputation, and operations.

We developed this Cyber Risk Scorecard based on combined analytics from your Cyber Threat Readiness Questionnaire responses and your risk rating. WhiteHawk presents key findings summarized as a prioritized list of options on which you can immediately act. All collected and analyzed open data sets are externally observable, and we do not conduct on premise or penetration testing of your company's internal networks with this scorecard.

- *Data-driven, dynamic measurements of an organization's, cybersecurity performance*
- *Derived from objective, verifiable information*
- *Material and validated measurements*
- *Created by a trusted, independent organization*

WhiteHawk designed the Cyber Risk Scorecard to provide clients with actionable information to:

- Facilitate budget-based and impactful, risk reduction decision-making based upon cyber risk vector indicators
- Enable timely actions
- Prevent online crime and fraud from disrupting business operations

WhiteHawk Cyber Analysts perform customized analytics to:

- Provide prioritized, affordable, and impactful options to mitigate cyber risks of small and midsize businesses and organizations
- Track key actions and mitigations to accept or address known risks
- Provide maturity planning in the form of an achievable risk reduction roadmap thereby enabling data-driven decision making in terms of business risk and budgets
- Maintain informed and enabling engagement

WHITEHAWK

Cyber Risk Scorecard Results Summary

We are pleased to present the results of the WhiteHawk Cyber Risk Scorecard. This section is an executive overview. Subsequent sections provide associated descriptions and context to our findings and solution options.

Company	Domain	# IP Addresses	Monitored by
Sample Company Inc.	Sample Company.com	3	3 Entities

Security Rating			Risk Vector Performance			
Ratings measure a company's relative security effectiveness.			*Risk Vector grades show how well the company is managing each risk vector.*			
770	Advanced:	900 – 740	Compromised Systems:	A	System Patching:	B
	Intermediate:	740 – 640	Communications Encryption:	A	Application Security:	A
	Basic:	640 – 250	User Behavior:	A	Email Security:	B
					Public Disclosure:	A

Prioritized Areas of Focus

WhiteHawk Cyber Analyst has identified top-3 Focus Areas the company should consider

Focus Area 1:	System Patching
Focus Area 2:	Email Security
Focus Area 3:	Compromised Systems

Solution Options

Solution options that address primary business risks identified in the Cyber Risk Scorecard. Alternatives for each are included in the product details section.

Essential Bundle	Balanced Bundle	Premier Bundle
– *Micro Focus Software Inc.: ZENworks Patch Management*	– *SecureMySocial: SecureMySocial for Individuals*	– *McAfee: McAfee Host Intrusion Prevention for Desktop perpetual license*
– *Acronis: Monitoring Service 1 Year*	– *Forcepoint Triton Software: SUREVIEW Insider Threat Endpoint Premium 36 month*	– *Virescit Tactical Systems: Information Assurance/ Cybersecurity*
	– *WireX Systems: WireX Systems NDR Platform*	– *Trusted Internet, LLC: Student Cyber Protector*
		– *Flexera Software: FlexNet Manager for Oracle*

For more solution options, visit www.whitehawk.com/marketplace

WHITEHAWK

Cyber Risk Scorecard Results Detail

Cyber Risk Security Rating Results

Cybersecurity Ratings, through BitSight Technologies, measure a company's security performance using a proprietary algorithm that analyzes externally observable data. Ratings range from 250 to 900 (analogous to consumer credit scores) with a higher rating equating to an overall better security posture with the ability to prevent cybercrime and fraud from impacting your business. In addition to gaining insight into your business's key cyber risks, companies can work with WhiteHawk Cyber Analysts to perform deeper analysis, including incorporating existing IT implementation baselines, to develop remediation strategies that align to your business model and objectives.

Cyber Risk Ratings are categorized as Basic, Intermediate, and Advanced. While different companies have differing methods of assessing risk, these categories serve as a general best practice guideline and marker of overall maturity of your cyber resilience.

Sample Company falls into the Advanced category, meaning its relative security effectiveness is high, having a strong security performance and lowest risk.

Industry Comparison: Sample Company. falls into the top 10% of the Technology industry.

Security Rating

770

Security Rating Categories and Approach

ADVANCED: 900 – 740
Relative security effectiveness is high, having a strong security performance and lowest risk

INTERMEDIATE: 740 – 640
Relative security effectiveness is fair, having an average security performance and medium risk.

BASIC 640 – 250
Relative security effectiveness is moderate, having a weak security performance and high risk.

Security Ratings are calculated using a proprietary risk measurement algorithm that evaluates evidence of security outcomes and practices. Multiple risk vectors comprise the rating, and it is updated daily. To provide a simple look at the external security posture of a company, the Security Rating is organized into three categories.

Cyber Security Risk Vector Results

As previously mentioned, security vectors and their outcomes are used to develop your personal Security Rating. In total, 23 risk vectors are used in the Risk Rating determination. For simplicity, we have organized them into seven (7) groups. Below describes each group and the company's associated resulting grade. We provide WhiteHawk's Cyber Analyst notes for additional context.

Risk Vector Performance *Risk Vector grades show how well the company is managing each risk vector.*	
Compromised Systems:	A
Communications Encryption:	A
User Behavior:	A
System Patching:	B
Application Security:	A
Email Security:	B
Public Disclosure:	A

A Compromised Systems

Compromised Systems risk vectors make up 55% of the Risk Rating. It contains information based on Botnet Infections, Spam Propagation, Malware Servers, Unsolicited Communications, and Potentially Exploited Devices. The total grade of all Compromised Systems risk vectors, configurations, and event durations factor into the entire Compromised Systems risk category. We then normalize them to account for company size.

WhiteHawk Cyber Analyst Notes:

- Your company is doing well in implementing best security practices. Continue improving policies and procedures to stay in the top 10% of companies within your industry.
- Sample Company for Compromised Systems is performing above average and is in the top 10% of companies within the same industry. Continue to ensure that local logging has been enabled on all systems and networking devices to monitor and track events to remain in the top percentile of your company's industry.

A Communications Encryption

Communications Encryption risk vectors analyze server configurations to determine if a server's security protocol libraries are correctly configured and supporting strong encryption when making connections to other machines. Incorrect configurations may make servers vulnerable to POODLE and Heartbleed attacks that can lead to attackers obtaining sensitive data. WhiteHawk checks TLS/SSL connections with servers and collects the certificate chain during the session negotiation process, allowing us to review and establish which hosts need updating.

WhiteHawk Cyber Analyst Notes:

- Your company is doing well in implementing best security practices. Continue improving policies and procedures to stay in the top 10% of companies within your industry.
- Sample Company for Communications Encryption is performing above average and is in the top 10% of companies within the same industry. Proper TLS/SSL certifications and configurations contribute to the current Communication Encryption. Continue to use proper TLS/SSL certifications and configurations to remain in the top percentile of your company's industry.

A User Behavior

User Behavior risk vectors focus on employee activities that may introduce risks into an organization's networks. User behavior risk examples include sharing files over BitTorrent and determining if employees are re-using corporate login credentials in external websites outside of the corporate network.

WhiteHawk Cyber Analyst Notes:

- Your company is doing well in implementing best security practices. Continue improving policies and procedures to stay in the top 10% of companies within your industry.
- Sample Company for User Behavior is performing above average and is in the top 10% of companies within the same industry. Content downloaded through file sharing services such as BitTorrent may be manipulated by malware authors. Downloading files without proper approval creates a risk of introducing malware to an organization's network. Continue or start conducting a gap analysis to understand the skills and behaviors of the workforce to and build a baseline education roadmap to remain in the top percentile of your company's industry.

B System Patching

System Patching risk vectors evaluate how vulnerabilities affect how many systems in an organization's network infrastructure and how quickly the company resolves any issues.

WhiteHawk Cyber Analyst Notes:

- Your company's performance is fair with light risk of an event occurrence. You are currently in the top 30% of companies within your industry which leaves opportunity to achieve best practices. Opportunities exist to build on the current policies in place on a quarterly basis to improve your security performance.
- Sample Company for System Patching is performing above average and is in the top 30% of companies within the same industry. Continue or start deploying automated software update tools to ensure that the operating systems are running the most recent security updates provided by vendors to remain in the top percentile of your company's industry.

A Application Security

Application Security risk vectors track security holes and liabilities introduced by out-of-date or unsupported server software and business applications. These vectors also track outgoing communications from desktop devices including metadata about the device's operating system and its browser version. WhiteHawk compares that information with currently released versions or software updates available for those systems.

WhiteHawk Cyber Analyst Notes:

- Your company is doing well in implementing best security practices. Continue improving policies and procedures to stay in the top 10% of companies within your industry.
- Sample Company for Application Security is performing above average and is in the top 10% of companies within the same industry. Continue or start tracking security holes and liabilities introduced by unauthorized operating systems and out-of-date or unsupported server software to remain in the top percentile of your company's industry.

B Email Security

Email Security risk vectors track the use of SPF, DKIM and DMARC DNS records. SPF on its own isn't enough to prevent domain name spoofing. Email has two possible “From” Address Fields (Envelope From, Header From.) SPF checks are done on the Envelope From, so it's not a preventative measure against all spoofing. Legitimate services do use this approach, for example, newsletters, but it is also used in spoofing. DKIM and DMARC both seek to get around this vulnerability. DKIM signs the email with a signature that a recipient server can verify against the Published DNS record. DMARC is used in conjunction with SPF; it aims to match the Header From domain name with the Envelope From used during the SPF check.

WhiteHawk Cyber Analyst Notes:

- Your company's performance is fair with light risk of an event occurrence. You are currently in the top 30% of companies within your industry which leaves opportunity to achieve best practices. Opportunities exist to build on the current policies in place on a quarterly basis to improve your security performance.
- Sample Company for Email Security is performing above average and is in the top 30% of companies within the same industry. Continue or start lowering the chances of spoofed or modified emails from valid domains by implementing the DMARC policy and verification to remain in the top percentile of your company's industry.

A Public Disclosure

Public Disclosure risk vectors are based on collected data breach information from verifiable news sources both domestic and international and by filing Freedom of Information Act (FOIA) requests. Information obtained through these research processes include a range of security events. Though these events do not necessarily result in direct data loss to you, the relevant interruptions to business continuity can be used to make informed decisions to improve your security preparedness.

WhiteHawk Cyber Analyst Notes:

- Your company is doing well in implementing best security practices. Continue improving policies and procedures to stay in the top 10% of companies within your industry.
- Sample Company for Public Disclosure is performing above average and is in the top 10% of companies within the same industry. Continue or start lowering the chances of spoofed or modified emails from valid domains by implementing the DMARC policy and verification to remain in the top percentile of your company's industry.

Path to CMMC: Your Alignment

What is CMMC?

CMMC stands for Cybersecurity Maturity Model Certification, a cyber risk maturity framework for all companies and organizations to follow to smartly prevent and mitigate a breadth of risks from cybercrime, fraud, espionage, and disruption. The U.S. Department of Defense (DoD) has started to incorporate CMMC certification into the Defense Federal Acquisition Regulation Supplement (DFARS) and use it as a standing requirement for contract award beginning in 2020. CMMC is based upon five maturity levels that range from "Basic Cybersecurity Hygiene" to "Advanced/Progressive."

Official Background Information:

- Home Page: Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification
- CMMC V1.0 OSD Public Briefing Slides
- CMMC V1.02 Official Document - PDF

Who Needs CMMC?

CMMC is starting to be leveraged to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB) and eventually all Federal contractors. The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene. The CMMC approach also attempts to protect controlled unclassified information (CUI) that resides in the Department's industry partners' networks.

What is WhiteHawk's "Path to CMMC" and Your Alignment?

WhiteHawk's maturity models were initially built upon the Center for Internet Security (CIS) Framework, which maps to the NIST Framework and is meaningful down to the midsize to small business levels. Using WhiteHawk's online maturity models, we have mapped the CIS Framework to CMMC. By aligning multiple frameworks, WhiteHawk can deliver an easy to understand and documented path to CMMC compliance.

What Level Does My Company Need to Achieve?

CMMC Levels are mapped to the work your company does. DOD expects the majority of subcontractors to prime DoD contractors to be at Level 1 and 2. An organization that handles CUI will need to achieve Level 3 and above.

Your Mapping to CMMC

WhiteHawk helps you map to CMMC using CIS Controls® tools mapped to the CMMC levels. CMMC's five different certification levels reflect the maturity and reliability of a government contractor's cybersecurity infrastructure to protect sensitive and high-level government information. The five levels (L1 – L5) build upon each other's technical requirements with the next level including the requirements from the previous level. See the visual below to better understand where each CIS control maps to these new standards.

CIS Control	#	CMMC Maturity Levels			
		L1	L2	L3	L4/5
Penetration Tests and Red Team Exercises	#20				-
Email and Web Browser Protections	#7			●	●
Limitation and Control of Network Ports, Protocols, & Services	#9			-	-
Application Software Security	#18			-	-
Inventory and Control of Software Assets	#2		●	●	●
Continuous Vulnerability Management	#3		-	-	-
Controlled Use of Administrative Privileges	#4		●	●	●
Maintenance, Monitoring and Analysis of Audit Logs	#6		-	-	-
Data Recovery Capabilities	#10		-	-	-
Secure Configuration for Network	#11		●	●	●
Implement a Security Awareness and Training Program	#17		-	-	-
Incident Response and Management	#19		-	-	-
Inventory and Control of Hardware Assets	#1	●	●	●	●
Secure Configuration for Hardware and Software	#5	●	●	●	●
Malware Defenses	#8	●	●	●	●
Boundary Defense	#12	●	●	●	●
Data Protection	#13	-	-	-	-
Controlled Access Based on the Need to Know	#14	●	●	●	●
Wireless Access Control	#15	●	●	●	●
Account Monitoring and Control	#16	●	●	●	●
		7/8	**10/16**	**11/19**	**0/20**

● *Meets or Exceeds All Expectations.* ● *Meets Some Expectations.* ● *Has Significant Shortfalls.* '-' *Insufficient Data.*

Recommendations

WhiteHawk Cyber Analysts analyzed the security rating and risk vector performance results and provide the following tailored solution options to prevent and mitigate online crime and fraud thereby improving your company's overall cybersecurity posture. We base the solution options on externally available information about cyber resilience gaps. Internal processes and IT solutions currently in place may impact company actions. WhiteHawk presents this information to provide areas of focus for further investigation and potential action. Please go to www.whitehawk.com to schedule an appointment with one of our Cyber Analysts to further refine, prioritize, and take smart actions to mitigate your leading cyber risks.

Top 3 Areas of Focus

Understanding and addressing cyber risks to your revenue, reputation, and operations can be overwhelming to a majority of businesses and organizations today. WhiteHawk has taken the results of your cyber risk rating and performed additional analysis to present a prioritized list of affordable and impactful solution options for you to consider as a starting point. Today and into the future, prevention of online crime and fraud and the protection of your company's and clients' sensitive information is an ongoing business need requiring an active and ongoing maturity approach. Take smart action now, starting with the following focus areas based on the perceived risks derived from the risk rating and risk vector assessment:

Focus Area 1: System Patching

Your company's performance is fair with light risk of an event occurrence. You are currently in the top 30% of companies within your industry which leaves opportunity to achieve best practices. Opportunities exist to build on the current policies in place on a quarterly basis to improve your security performance.

Focus Area 2: Email Security

Your company's performance is fair with light risk of an event occurrence. You are currently in the top 30% of companies within your industry which leaves opportunity to achieve best practices. Opportunities exist to build on the current policies in place on a quarterly basis to improve your security performance.

Focus Area 3: Compromised Systems

Your company is doing well in implementing best security practices. Continue improving policies and procedures to stay in the top 10% of companies within your industry.

WHITEHAWK

Solution Options

In alignment with the above focus areas, WhiteHawk presents three bundled solution options for your company's consideration. Please schedule a quick call with one of our Cyber Analysts to refine and select the best options for your needs and business priorities. This process starts your cybersecurity maturity journey in context to your company's current IT implementation processes and implementations.

WhiteHawk presents three solution options with alternatives for each category for your consideration.

The Essential Bundle provides the **essential** cybersecurity products that fit your company's immediate cyber risk needs based on the Cyber Threat Readiness Questionnaire results and cyber risk rating. This bundle represents the minimum your company needs to be doing to **prevent or mitigate the most common cybercrime and fraud events**.

ESSENTIAL BUNDLE

BALANCED BUNDLE

The Balanced Bundles offers the cybersecurity products and services that represent the **standard best practices for your company's online operations.** This bundle is comprised of key solution options for your business to address your priority cyber risks.

The Premier Bundles provides **top of the line maturity level** for cybersecurity products. This bundle represents the level of cyber maturity that your company should be **striving towards to address a wide range of cybercrime and fraud vectors threatening your revenue, customers, and reputation.**

PREMIER BUNDLE

WHITEHAWK

ESSENTIAL BUNDLE

Patch Management

Micro Focus Software Inc. — ZENworks Patch Management		Flexera Software — Personal Software Inspector
Defend your network against the high costs of viruses. Micro Focus ZENworks® Patch Management (formerly Novell® ZENworks Patch Management) is an automated patch management solution that retrieves and deploys the right patches to the right machines at the right times.	*or*	Personal Software Inspector is a free computer security solution that identifies vulnerabilities in applications on your private PC. Vulnerable programs can leave your PC open to attacks, against which your antivirus solution may not be effective. Simply put, it scans software on your system and identifies programs in need of security updates to safeguard your PC against cybercriminals. It then supplies your computer with the necessary software security updates to keep it safe.

Network Discovery

Acronis — Monitoring Service 1 Year		GFI Software — LanGuard 1 Year
A SaaS-based unified monitoring solution for cloud, on-premise, and hybrid infrastructures. Acronis Monitoring Service offers full stack monitoring that includes servers and VMs, applications, networks, services, websites, processes, and more.	*or*	GFI LanGuard provides a complete network security overview with minimal administrative effort, while also providing remedial action through its patch management features.

BALANCED BUNDLE

Web Filter

SecureMySocial — SecureMySocial for Individuals		SecureMySocial — SecureMySocial for Businesses
SecureMySocial helps people protect themselves from the personal and professional damage that can occur from problematic social media posts (made by themselves or by others referencing them) by providing real-time warnings as problematic material is posted so as to ensure immediate removal.	*or*	SecureMySocial protects businesses from the potentially catastrophic consequences of problematic material posted to social media. SecureMySocial provides real-time warnings to employees if they or their contacts post such items on social media sites such as Facebook and Twitter. SecureMySocial's facilitation of quick removal both contains damage and helps shield a firm in case of lawsuits or regulatory investigations.

Traffic Analysis

Forcepoint Triton Software — SUREVIEW Insider Threat Endpoint Premium 36 month		Trend Micro — Deep Discovery Inspector
Forcepoint Insider Threat identifies the riskiest insiders in your environment and empowers your teams to confidently investigate and remediate the threat. Forcepoint combines User visibility, advanced analytics, DLP integration and security orchestration for complete User behavior monitoring. By focusing on peoples' interactions with data, Forcepoint Insider Threat prevents behavioral-based data loss and exposes other insider threats that present risk to critical systems, such as fraudulent transactions or cyber sabotage.	*or*	Deep Discovery Inspector is available as a physical or virtual network appliance. It's designed to quickly detect advanced malware that typically bypasses traditional security defenses and exfiltrates sensitive data. Using specialized detection engines and custom sandbox analysis, breaches can be detected and prevented.

Incident Response

WireX Systems — WireX Systems NDR Platform		Votiro — Incident Manager
We deliver comprehensive security intelligence in actual human readable form so you can save effort and time when validating alerts and responding to security incidents.	*or*	Votiro offers you a state-of-the-art Incident Manager that enables you to easily control scanning and neutralization process in your organization.

WHITEHAWK

PREMIER BUNDLE

Host-Based Intrusion Prevention System

McAfee — McAfee Host Intrusion Prevention for Desktop perpetual license		Check Point — Threat Prevention Security Suite
McAfee Host Intrusion Prevention safeguards businesses against complex security threats that may otherwise be unintentionally introduced or allowed by desktops, laptops, and servers. It leverages a three-part threat defense — signature analysis, behavioral analysis, and system firewall — all easily managed from one central console, the McAfee ePolicy Orchestrator (ePO) platform..	*or*	Increasing your enterprise security often means increasing your complexity and management challenges in kind. Check Point delivers a multi-layered line of defense to help you maximize your security while minimizing challenges and closing gaps.

Security Information and Event Management

Virescit Tactical Systems — Information Assurance/ Cybersecurity		Virescit Tactical Systems — Information Assurance/ Cybersecurity
We are dedicated to the advancement of defense technologies in order to save future lives on the battlefield and ensure the safety and security of the information of the United States.	*or*	We are dedicated to the advancement of defense technologies in order to save future lives on the battlefield and ensure the safety and security of the information of the United States.

— Premier Bundle Solution Options Continued on Next Page —

PREMIER BUNDLE - CONTINUED

Managed Security Services

Trusted Internet, LLC — Student Cyber Protector

With Trusted Internet, you get: Online transparent protection - we protect your kids while they're online. If we find a problem, we troubleshoot it remotely and can, many times, block the application or website from being accessed again. If the problem is bigger than that, we can respond onsite in your home, clean computers, fix malware and stop the problem from happening again. Imagine allowing kids more freedom online, knowing that they're being protected --and they don't even know it. Now imaging being able to know the applications, web sites and security threats that they face online. And then, that a professional team of security operators are keeping them safe.

or

Cyber BDA — Cyber Sales Force TRAINING

Our sales-focused TRAINING services offers added value to your client and partner network. This service empowers your team with knowledge of how your cyber products and services are applied to Federal government customer requirements. As an example, we tailor our introductory class to focus on cyber.

Compliance Reporting

Flexera Software — FlexNet Manager for Oracle

FlexNet Manager for Oracle is a scalable Oracle license compliance and Software License Optimization solution that is built on the FlexNet Manager Platform. FlexNet Manager for Oracle automates and optimizes license management to enable the reduction of license, maintenance and audit costs for Oracle software, while maintaining license compliance.

or

iTrust — Risk Management Suite - 25 Vendors

iTrust provides cybersecurity risk ratings and risk intelligence to help businesses build trusted relationships with their vendors, partners, and suppliers. iTrust is an all-in-one platform with the essential risk management capabilities businesses in today’s environment need.

About Us

Easily find out where the biggest risks are

In near real time make the changes you need to protect your organization

Get alerted to new threats that are targeting you

Track how your network vulnerabilities change over time

WhiteHawk, Inc., is the first online Cybersecurity Exchange based on a platform architecture that is Artificial Intelligence (AI)-driven, with a focus on identifying, prioritizing, and mitigating cyber risks for businesses of all sizes. WhiteHawk continually vets and assesses risk-focused technologies, methodologies, and solutions that are impactful, affordable, and scalable to stay up to date on current cyber threat vectors to businesses, organizations, family offices, and individuals. We have an online approach to determining your key cyber risks through a Cyber Threat Readiness Questionnaire, and as appropriate, a cyber risk assessment. Using this information, we then match tailored risk mitigation solution options to companies and organizations based on current threat trends across key sectors. Our Cyber Consultants on staff help build a tailored cyber maturity plan customized to meet your business or mission objectives.

For more information, visit www.whitehawk.com.

WhiteHawk CEC, Inc.
Terry Roberts - Founder, President, & CEO
consultingservices@whitehawk.com

WHITEHAWK

Disclaimer for Cyber Risk Scorecard

The Cyber Risk Scorecard and its contents and use are expressly subject to the WhiteHawk Terms and Conditions contained at https://www.whitehawk.com/terms-conditions. Acceptance of this Cyber Risk Scorecard, or use of any information contained herein, by any party receiving this Cyber Risk Scorecard (each "Recipient") shall constitute an acknowledgement and acceptance by such Recipient of, and agreement by such Recipient to also be bound by, the following:

Background: WhiteHawk's proprietary open analytic approach to understanding the cyber risk landscape globally, tracking threat vectors that impact each Public and Private Sector, and mapping to discoverable risk activity being experienced by a specific organization or company result in a current (and therefore dynamic) cyber risk profile based upon vetted and published risk standards and frameworks (including, but not limited to the Center for Internet Security [CIS]/National Institute of Standards and Technology [NIST]/Cybersecurity Maturity Model Certification [CMMC]). All identified risk data sets, impacting a specific company or organization with a uniquely registered internet domain address, are then prioritized and mapped to key areas of focus and potential risk mitigation options, in a tailored and easy to understand and actionable Cyber Risk Scorecard.

(1) This Cyber Risk Scorecard was created by WhiteHawk CEC Inc. for the entity named herein (the "Company") and is based on publicly accessible information, not within the control of WhiteHawk. In preparing this Cyber Risk Scorecard, WhiteHawk has conducted cyber risk analytics that are assumed to be as complete and correct as an external assessment can be. In preparing this Cyber Risk Scorecard, the WhiteHawk platform and team leverages a broad set of publicly available cyber risk related data sets and cyber threat information regarding companies, organizations, vendors, and suppliers. When WhiteHawk is given permission to work directly with companies then additional Digital Footprint information can be voluntarily provided via the WhiteHawk online Cyber Threat Readiness Questionnaire and a virtual consult, which additional information is then incorporated into an updated Cyber Risk Scorecard. As a result of the foregoing and the nature of Digital Age Risk, WhiteHawk stands behind the use of Its Cyber Risk Scorecard to prioritize discoverable risks and to make initial vetting decisions. Cyber risks, however, can only be conclusively validated by a Red Team or on-premise sensors or inspection. The information contained in this Cyber Risk Scorecard is a guideline based upon publicly available risk indicators and proven risk standards and best practices and is a sound basis for formulating an initial risk mitigation plan. Cyber risk and fraud can be smartly reduced but cannot be completely prevented nor eliminated.

(2) TO THE FULLEST EXTENT PERMITTED BY LAW, WHITEHAWK'S TOTAL LIABILITY, ON A CUMULATIVE AND AGGREGATE BASIS, TO THE COMPANY AND ALL RECIPIENTS AND OTHER PARTIES, RESULTING FROM WHITEHAWK'S ACTIONS IN RELATION TO THE CREATION AND DISSEMINATION OF THIS CYBER RISK SCORECARD, WILL BE LIMITED TO THE AMOUNT OF COMPENSATION ACTUALLY RECEIVED BY WHITEHAWK FROM THE COMPANY FOR THE CREATION OF THIS CYBER RISK SCORECARD.

IF ANY RECIPIENT IS NOT WILLING TO ACKNOWLEDGE AND ACCEPT, OR AGREE TO, THE TERMS SET FORTH ABOVE, IT MUST RETURN THIS CYBER RISK SCORECARD TO WHITEHAWK IMMEDIATELY WITHOUT MAKING ANY COPIES THEREOF, EXTRACTS THEREFROM OR USE (INCLUDING DISCLOSURE) THEREOF. A RECIPIENT'S FAILURE SO TO RETURN THIS CYBER RISK SCORECARD SHALL CONSTITUTE ITS ACKNOWLEDGEMENT AND ACCEPTANCE OF AND AGREEMENT TO THE TERMS SET FORTH ABOVE.

Cyber Risk Scorecard

WhiteHawk CEC, Inc.

www.whitehawk.com