WHITEHAWK

Cyber Risk Scorecard — Snapshot

For Company: Sample Company

Prepared on:

January 6, 2021

Table of Contents

WhiteHawk Cyber Risk Scorecard — Snapshot

WhiteHawk's Cyber Risk Scorecard — Snapshot provides businesses and organizations a cyber risk profile which informs clients of key risks to their revenue and reputation by providing actionable options to prevent and mitigate online crime, fraud, and disruption. We partner with you through our Cyber Risk Journey to baseline, understand, review, and act to decrease the likelihood of your company becoming a victim and to reduce the impact of any cyber event. Below summarizes the activities we perform with you. We document this all in the summary of your Cyber Risk Profile report.

Baseline

Cyber Threat Readiness Questionnaire

Do you need to worry about cybersecurity and cyber risk? By responding to ten, non-intrusive questions about your company, WhiteHawk is able to calculate a risk and complexity score using Artificial Intelligence (AI)-based approaches to determine the likelihood of your company or organization becoming victim to cyberattacks. Using the resulting risk and complexity score, we baseline your cyber risk profile by assessing reported cyber events and crimes (breaches, malware etc.) that have impacted both your sector and companies of similar size and complexity, thereby providing a focused risk profile of your company.

Understanding

Cyber Risk Consultation

What does it all mean? Through a complimentary 20-minute virtual consultation with one of our Cyber Analysts, we review with you the results of the Cyber Threat Readiness Questionnaire and the solution options that can strengthen your cyber risk posture.

Review

Cyber Risk Maturity — Assessment

How do I prioritize my limited resources? WhiteHawk leverages the Center for Internet Security (CIS) Critical Security Controls for Effective Cyber Defense best practice guidelines to provide solution options. We address prioritized areas of weakness particular to your business's profile.

Action Plan

Cyber Risk Maturity — Action Planning

Where do I start? Because the CIS Critical Security Controls can appear technical, WhiteHawk's Cyber Analyst works with you to break down each affordable, actionable step of your Action Plan. As you take each step, we review and discuss potential next actions, each as part of your Cyber Risk Journey.

Cyber Risk Profile — Cyber Threat Readiness Questionnaire

Through the use of ten, non-intrusive questions, we use our proprietary algorithms to calculate your company's risk and complexity score within a specific industry. We then provide a comparative analysis of how companies of similar size and complexity have fared against the current cybercrime and fraud environment. Below summarizes your most recent responses to our Cyber Threat Readiness Questionnaire.

#	QUESTION	RESPONSE
1	In which industry is your business?	Professional
2	How many employees does your company have? Include all full time, part time, and contractors.	12
3	How many users are on your company network? In many cases, this will be the same as the total number of employees.	10
4	How many office locations does your company have?	1
5	How many company-issued devices (cell phones, computers, iPads, tablets, servers, etc.) does your company own?	6
6	How extensively does your company use cloud-based services?	None
7	What type of client interactions do you have?	Email
8	How much web traffic do you receive?	Low
9	How much knowledge do your information technology (IT) security personnel have of IT security issues?	None
10	How much of your IT support personnel can provide skilled operational support for the company's networking needs?	None

Cyber Risk Profile — Risk Indicator Synopsis

The Cyber Risk Indicator below provides insight and awareness of how companies or organizations of similar size and complexity have been impacted by cybercrime and fraud over the past year. Based upon the size and complexity score derived from your answers to our Cyber Threat Readiness Questionnaire, we are able to assess and review cyber events that have been reported across the same industry or sector. This comparison provides context to the mapping of key cybersecurity solutions to your protection priority needs. The indicator pointing to red equates to a significant number of companies like yours having experienced online crime and fraud events in the past year. Below is a synopsis of our findings.

Cyber Risk Indicator

Based on the answers provided, your focus should be on providing basic cybersecurity without spending too much of the company's resources - manpower and money. Small businesses are popular cybercrime targets because many have not implemented basic protections. While most cyber criminals won't target your business explicitly, they will launch relatively simple attacks against everyone they can find. Typically, cyber criminals targeting small businesses plan to use the data they steal to commit financial fraud. By making your security posture significantly better than that of the average small business, you can largely escape the attackers' notice. They will instead move on to softer targets. In addition, attackers may see you as a useful stepping-stone in attacking your business partners.

Your company tends toward light, informal internal rules. Because of this, you should make sure that you have appropriate plans in place to deal with cybersecurity breaches. It is important to know and understand your risks in order to take appropriate steps to mitigate them. You should set up employee training and controls on your corporate network to ensure employees are equipped with the knowledge to identify and report potential scams. In addition, developing an incident response plan will help your company respond and recover if and when it is attacked and will help to protect your reputation.

Our evaluation indicates that your current overall cybersecurity posture is poor. Your company needs to take immediate steps to close the most urgent gaps in your cybersecurity.

This profile is based on the small amount of business-specific data you have provided through the questionnaire, and on broad statistics for your industry. Please contact WhiteHawk to get a more accurate, personalized evaluation.

Cyber Risk Maturity Roadmap — Maturity Level Assessment

WhiteHawk knows that learning about, prioritizing, and mitigating Digital Age Risks is a continuous journey that all companies and organizations, no matter the size, have an inherent interest and responsibility to undertake to protect their reputations, revenue, and key data assets. The cyber landscape moves at the speed of technology, with cyber criminals and bad actors finding new and innovative ways to steal and disrupt. Your cyber risk strategy and priorities must keep pace or fail.

To prioritize your Roadmap, we use the CIS Critical Security Controls to baseline and track your company's progress and maturity toward mitigating your key risks. The CIS Critical Security Controls, which align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, were designed to create a common language for managing risk within a company. It is comprised of 20 best practices that help guide you through the process of creating and managing a cybersecurity strategy. Research has demonstrated that implementing the CIS Critical Security Controls can effectively mitigate the key risks from online crime, fraud, and disruption by as much as 85%.

The 20 controls are organized into three implementation groups in order to guide you through your cybersecurity journey. The virtual consultations with our Cyber Analysts provide a baseline of your current cyber focused solutions and processes. We then develop, track, and maintain a maturity roadmap, thereby increasing your resilience to a breadth of cyberattacks. We summarize the CIS Critical Security Control groups, and their features and attributes below. Visit us at www.whitehawk.com to schedule your cyber consult today.

BASIC IMPLEMENTATION GROUP	FOUNDATIONAL IMPLEMENTATION GROUP	ORGANIZATIONAL IMPLEMENTATION GROUP
– Identifying the Security Environment - aka "cyber hygiene" – For organizations with limited resources and experts to implement controls – Focused on understanding the people, software, and devices that have access to client/proprietary data	– Protecting Assets – For organizations with moderate resources and experts to implement controls – Advanced guidance to improve the technical aspects of security – Focused on the technical security controls used to conduct its processes – Email and Browsers, Malware and Viruses, Networks, Boundaries, Data, Wireless, and Account Controls	– Developing a Security Culture – For mature organizations with significant resources and experts to implement controls – Focused on the people and associated processes o Security Awareness Training o Security Lifecycle of Software o Incident Response o Penetration Testing

Cyber Risk Maturity Roadmap — CIS Critical Security Controls Implementation Tracking

Through either self-service or via our Cyber Analyst consults, we map the CIS Critical Security Controls as appropriate to your company profile. Visit www.whitehawk.com to update your Roadmap progress and to schedule a consult with our Cyber Analysts and dig into impactful, affordable, and easy to implement solution options that best meet your needs. The below represents your current implementation status of the CIS Critical Security Controls.

CIS CRITICAL SECURITY CONTROLS & IMPLEMENTATION GROUPS

BASIC IMPLEMENTATION CONTROLS	
✓	Inventory and Control of Hardware Assets
✓	Inventory and Control of Software Assets
x	Continuous Vulnerability Management
✓	Controlled Use of Administrative Privileges
✓	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
x	Maintenance, Monitoring and Analysis of Audit Logs
x	Email and Web Browser Protections
FOUNDATIONAL IMPLEMENTATION CONTROLS	
✓	Malware Defenses
✓	Limitation and Control of Network Ports, Protocols, and Services
x	Data Recovery Capabilities
✓	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
✓	Boundary Defense
x	Data Protection
x	Controlled Access Based on the Need to Know
x	Wireless Access Control
x	Account Monitoring and Control
ORGANIZATIONAL IMPLEMENTATION CONTROLS	
x	Implement a Security Awareness and Training Program
x	Application Software Security
✓	Incident Response and Management
x	Penetration Tests and Red Team Exercises

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.

Path to CMMC: Your Alignment — Continued

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				x
Email and Web Browser Protections	#7			x	x
Limitation and Control of Network Ports, Protocols, & Services	#9			✓	✓
Application Software Security	#18			x	x
Inventory and Control of Software Assets	#2		✓	✓	✓
Continuous Vulnerability Management	#3		x	x	x
Controlled Use of Administrative Privileges	#4		✓	✓	✓
Maintenance, Monitoring and Analysis of Audit Logs	#6		x	x	x
Data Recovery Capabilities	#10		x	x	x
Secure Configuration for Network	#11		✓	✓	✓
Implement a Security Awareness and Training Program	#17		x	x	x
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	x	x	x	x
Controlled Access Based on the Need to Know	#14	x	x	x	x
Wireless Access Control	#15	x	x	x	x
Account Monitoring and Control	#16	x	x	x	x
		4/8	**8/16**	**9/19**	**9/20**

Cyber Risk Maturity Roadmap — Prioritized Action Plan

WhiteHawk understands that for some businesses the CIS Critical Security Controls can appear technical and daunting. This is especially the case for those organizations that do not have advanced experience and expertise in IT and cybersecurity. To help create an easy to implement action plan you can prioritize based on budget and business objectives, we help translate the CIS Critical Security Controls into actionable taskings. Through our virtual consult, we review your Cyber Risk Profile (based on the Cyber Threat Readiness Questionnaire) and discuss additional details of current IT and security approaches. We work with you to develop a prioritized action plan that aligns to the CIS Critical Security Controls to manage and track the maturity of your company over time. For companies that have in-house expertise, our www.whitehawk.com platform also allows for self-service tracking of both the CIS Critical Security Controls and the Prioritized Action Plan as a part of your overarching Cyber Risk Maturity Roadmap.

To help organize and prioritize your implementation progress, we group the Actions into three categories:

- **Critical Actions**: These represent the highest priority actions that should be taken by the organization as soon as possible. Most times, these actions are simple and affordable while making significant impact on the overall security posture for your company's revenue, reputation, and operations.
- **Next Actions**: Once the most critical actions are implemented, Next Actions represent the tasking that will start your maturity journey to improving the protection of your most critical data sets.
- **Pending Actions**: The last set of Pending Actions reflect achieving the highest level of maturity that is applicable for your business sector. Important to note that the cyber landscape is everchanging, so ensuring a semi-annual or an annual review cycle to reassess your security posture will enable your company to stay ahead of new digital fraud and crime schemes and methods impacting your sector.

Below is your current Action Plan. There may be additional actions in your profile, so visit your account profile on www.whitehawk.com to view the complete list.

ACTION PLAN CUSTOMIZED FOR YOUR COMPANY

CRITICAL ACTIONS	
x	Audit Log Collection
x	Email and Web Browser Protections
x	Wireless Access Control
NEXT ACTIONS	
x	Data Protection
x	Account Monitoring and Control
PENDING ACTIONS	
x	Implement a Security Awareness and Training Program

Cybersecurity Solution Bundles

Using the responses from the Cyber Threat Readiness Questionnaire, WhiteHawk presents three bundled solution options for your company's or organization's consideration. Because this is solely reflective of the high-level questions and does not take into consideration your company's current IT solutions and business practices, we highly recommend you schedule a quick call with one of our Cyber Analysts to refine and select the best options for your needs and business priorities. Visit www.whitehawk.com to schedule a complimentary 20-minute consultation today.

ESSENTIAL BUNDLE

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**.

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.

PREMIER BUNDLE

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 toward to address a wide range of cybercrime and fraud vectors threatening your revenue, customers, and reputation.**

Cybersecurity Solution Bundles — Continued

WhiteHawk leverages the complexity score results of our Cyber Threat Readiness Questionnaire to tee up solution options available through our online Marketplace. Our Marketplace offers hundreds of solutions with multiple options to choose from, based on the business size and its cyber risk objectives. Below lists the solution categories that are applicable to your business using the complexity score. Because of the multiple options available for each category, please visit www.whitehawk.com to learn more of the products available and schedule a consult with one of our Cyber Analysts to take the next steps in your Cyber Risk Journey. The following section provides definitions for each solution category as reference.

Essential Bundle	Balanced Bundle	Premier Bundle
Access Control	Access Control	Access Control
Antimalware	Antimalware	Antimalware
Backup	Backup	Backup
Email Filter	Compliance Reporting	Compliance Reporting
Encrypted Storage	Email Filter	Email Filter
Web Services Security	Encrypted Storage	Encrypted Storage
	Host-Based Intrusion Prevention System	Forensics
	Patch Management	Host-Based Intrusion Prevention System
	Security Information and Event Management	Patch Management
	Training	Security Information and Event Management
	Virtual Private Network	Threat Intelligence
	Web Services Security	Traffic Analysis
		Training
		Virtual Private Network
		Web Services Security

Solution Category Definitions

Solution Category	Definition
Access Control	The selective restriction of access to a place or other resource while access management describes the process. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization.
Antimalware	Software that protects the computer from malware such as spyware, adware, and worms. It scans the system for all types of malicious software that manage to reach the computer. An anti-malware program is one of the best tools to keep the computer and personal information protected.
Application Security	Products that monitor for security holes and liabilities introduced by out-of-date or unsupported server software.
Backup	A copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event.
Compliance Reporting	Reports that show you are following those procedures to insulate you from a potential audit by a regulatory organization. Failure to pass such an audit could damage reputation and result in downtime while non-compliant systems are brought up to standard.
Data Leak Prevention	Data loss prevention software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting, and blocking sensitive data while in use, in motion, and at rest.
Denial of Service Mitigation	Distributed denial-of-service (DDoS) mitigation is a set of techniques or tools for resisting or mitigating the impact of distributed denial-of-service attacks on networks attached to the Internet by protecting the target and relay networks.
Email Filter	Email filtering is the processing of email to organize it according to specified criteria. Filters can be set to quarantine suspicious emails that contain spam or other malicious kinds of files depending on the restrictions.
Encrypted Communication	Encryption is a method in which data is rendered hard to read by an unauthorized party. Since encryption methods are created to be extremely hard to break, many communication methods either use deliberately weaker encryption than possible, or have backdoors inserted to permit rapid decryption.
Encrypted Storage	Storage encryption is the use of encryption/decryption of backed-up and archived data, both in transit and on storage media.
Forensics	Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.
Host-based Intrusion Prevention System	A host-based intrusion prevention system (IPS) is an intrusion detection system that is capable of monitoring and analyzing the internals of a computing system as well as the network packets on its network interfaces, similar to the way a network-based intrusion detection system operates.
Incident Response	Incident response is a term used to describe the process by which an organization handles a data breach or cyber attack, including the way the organization attempts to manage the consequences of the attack or breach (the “incident”). Ultimately, the goal is to effectively manage the incident so that the damage is limited and recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.

Solution Category Definitions — Continued

Solution Category	Definition
Insider Threat Analytics	Monitor what users are doing in real-time, particularly those with elevated privileges such as system administrators and workers with access to highly sensitive information like trade secrets, intellectual property, or customer account data. Insider Threat Analytic products look for behaviors that are outside the range of normal activities to detect rogue insiders or external intruders who have compromised a user's account.
Malware analysis	Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, Trojan horse, rootkit, or backdoor.
Managed Security Services	Functions of a managed security service include round-the-clock monitoring and management of intrusion detection systems and firewalls, overseeing patch management and upgrades, performing security assessments and security audits, and responding to emergencies
Network discovery	Network discovery determines whether other computers and devices connected to the network can see and communicate with each other. When enabled on your personal computer (PC), you'll be able to see other computers and devices connected to the same network.
Network Intrusion Detection System	Network-based intrusion detection systems (NIDS) are devices intelligently distributed within networks that passively inspect traffic traversing the devices on which they sit. NIDS can be hardware or software-based systems and, depending on the manufacturer of the system, can attach to various network mediums such as Ethernet, Fiber Distributed Data Interface (FDDI), and others.
Network Intrusion Prevention System	An IPS is a form of network security that works to detect and prevent identified threats. Intrusion prevention systems continuously monitor your network looking for possible malicious incidents and capturing information about them.
Orchestration	Security orchestration is making different products (both security and non-security) integrate with each other and automating tasks across products through workflows while also allowing for end user oversight and interaction. Security automation is a subset of security orchestration.
Patch Management	Patch management is the process that helps acquire, test, and install multiple patches (code changes) on existing applications and software tools on a computer enabling systems to stay updated on existing patches and determining which patches are the appropriate ones.
Physical Security	Physical security is the protection of personnel, hardware, software, networks, and data from physical actions and events that could cause serious loss or damage to an enterprise, agency, or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism, and terrorism.
Secure Managed File Transfer	Managed file transfer (MFT) refers to a software or a service that manages the secure transfer of data from one computer to another through a network (e.g., the Internet). MFT software is marketed to corporate enterprises as an alternative to using ad-hoc file transfer solutions, such as file transfer protocol (FTP), hypertext transfer protocol (HTTP). and others.

Solution Category Definitions — Continued

Solution Category	Definition
Security Information & Event Management	Security Information and Event Management (SIEM) is a set of tools and services offering a holistic view of an organization's information security. SIEM correlates events gathered from different logs or security sources, using if-then rules that add intelligence to raw data.
Security Network Engineering	Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.
Threat Intelligence	Cyber threat intelligence is information about threats and threat actors that helps mitigate harmful events in cyberspace. Sources include open source intelligence, social media intelligence, human Intelligence, technical intelligence, or intelligence from the deep and dark web.
Threat Manager	Threat Manager protects your hybrid infrastructure, applications, and cloud workloads. It combines a network intrusion detection system (IDS) with vulnerability management into a single managed security-as-a-service.
Traffic Analysis	Traffic analysis is the process of intercepting and examining messages to deduce information from patterns in communication which can be performed even when the messages are encrypted.
Training	Security awareness training is a formal process for educating employees about computer security. A good security awareness program should educate employees about corporate policies and procedures for working with information technology.
Virtual Private Network	A Virtual Private Network is a service that allows you to connect to the Internet via an encrypted tunnel to ensure your online privacy and protect your sensitive data. A VPN is commonly used to secure connection to public Wi-Fi hotspots, hide IP addresses, and make your browsing private.
Virtualization Security Endpoint Protection	Security virtualization is the shift of security functions from dedicated hardware appliances to software that can be easily moved between commodity hardware or run in the cloud. Endpoint protection refers to a system for network security management that focuses on network endpoints, or individual devices such as workstations and mobile devices from which a network is accessed.
Vulnerability Assessment	A vulnerability assessment is the process of defining, identifying, classifying, and prioritizing vulnerabilities in computer systems, applications, and network infrastructures and providing the organization being assessed with the necessary knowledge, awareness, and risk background to understand the threats to its environment and react appropriately.
Web Filter	A web filter, which is commonly referred to as "content control software", is a piece of software designed to restrict what websites a user can visit on his or her computer. Filters are often installed either as a browser extension, as a standalone program on the computer, or as part of an overall security solution.
Web Services Security	Web Services Security (WS Security) is a specification that defines how security measures are implemented in web services to protect them from external attacks. It is a set of protocols that ensure security for Simple Object Access Protocol (SOAP)-based messages by implementing the principles of confidentiality, integrity, and authentication.

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

Cyber Risk Scorecard Disclaimer

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 — Snapshot

WhiteHawk CEC Inc.

515 King Street, Suite 450, Alexandria, VA 22314

www.whitehawk.com

Contact Advisory Services at consultingservices@whitehawk.com or call (833) 942-9237

Copyright © 2020 WhiteHawk CEC, Inc. All Rights Reserved.