WHITEHAWK

Cyber Risk Scorecard

On Company: Mid-Size Data Management Company

Prepared for:

Prepared by:

Prepared on:

01 JULY 2019

The information presented here is for general informational purposes only. All information is provided in good faith; however, we make no representation or warranty of any kind, expressed or implied, regarding the accuracy, adequacy, validity, reliability, availability, or completeness of any information presented. Under no circumstances shall we have any liability to you for any loss or damage of any kind incurred as a result of the used of the information provided.

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 smart 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 focused options on which businesses can immediately act. All collected and analyzed open data sets are externally observable, and we do not conduct on premise or penetration testing of a company's internal networks with this scorecard.

WhiteHawk partners with BitSight Technologies to provide topline risk ratings and identify selective insight trends based on 23 risk controls to prioritize risk indicators for enterprises.

BITSIGHT®
The Standard in SECURITY RATINGS

- *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

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 recommendations.

Company	Domain	# IP Addresses
Mid-Size Data Management Company	www.test.com	19,610

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.*			
640	Advanced:	900 – 740	Compromised Systems:	B	Systems Patching:	C
	Intermediate:	740 – 640	Communications Encryption:	D	Application Security:	C
	Basic:	640 – 250	User Behavior:	A	Email Security:	C
					Public Disclosure:	A

Prioritized Areas of Focus *WhiteHawk Cyber Analyst recommendations for top-3 Focus Areas the company should consider*	
Recommended Focus Area 1:	Communications Encryption
Recommended Focus Area 2:	Application Security
Recommended Focus Area 3:	Email Security

Solution Options

Solution options that address primary business risks identified in the Cyber Risk Scorecard

Basic Bundle	Balanced Bundle	Advanced Bundle
- *Sophos: Sophos Email Protection* - *KnowBe4: 1 Year - Security Awareness Training*	- *Symantec: Symantec Desktop Email Encryption* - *StorageCraft: ShadowProtect IT Edition V5.x Subscription - 1 Year* - *Micro Focus Software Inc.: ZENworks Patch Management*	- *Forcepoint: SUREVIEW Insider Threat Core* - *Micro Focus Software Inc.: Sentinel Enterprise* - *Verodin: Security Implementation Platform (SIP)* - *D3 Security: D3 SOAR*

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' key cyber risks, companies can work with WhiteHawk Cyber Analysts to perform deeper analysis (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.

Mid-Size Data Management Company falls into the Intermediate category meaning its relative security effectiveness is fair, having an average security performance and medium risk.

Industry Comparison: Mid-Size Data Management Company is in the Bottom 30% of the Technology industry.

Security Rating

640

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 Rating 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:	B
Communications Encryption:	D
User Behavior:	A
Systems Patching:	C
Application Security:	C
Email Security:	C
Public Disclosure:	A

B 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'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 securityperformance.

— A big concern that been found is the amount of compromised systems due to botnet and potential exploited systems. Over the past 90 days there has been a total 33 events. The number of incidents is a high level of concern because machines can be infected and allow cybercriminals to connect and take control of systems. Majority of these events were infections through a family of malware that can give attackers remote access to infected devices. It is distributed through spam messages and infected removable storage devices.

D 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 has departed from best security practices which could lead to a moderate amount of risk. You are currently in the Bottom 40% of companies within your industry. Begin to review current policies and procedures to improve your company's security performance now.

— Due to improper TLS/SSL certifications and configurations, its current rating is decreasing significantly putting Mid-Size Data Management Company is in the bottom 30% of all companies. The result of this poor grade is from utilizing insecure protocols such as TLSv1.0 and TSLv1.1 Lastly your company is using shorter keypairs, Diffie- Hellman primes less than 2048 bits are estimated to be breakable by adversaries with nation- state-level resources. If this behavior continues your company will increase the risk on its security posture making it easier for actors to access sensitive data.

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.

C Systems Patching

Systems 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 is performing at an average level which increases the probability of an event occurring. You are currently in the Bottom 40% of companies within your industry. To improve your performance, ensure your company and your personnel follow current patching policies and procedures soon.
- Mid-Size Data Management Company is slower to remediate vulnerabilities with an average of 99 weeks to remediate.
  Over the last 90 days there has been an average of 28 attacks with POODLE and DROWN being the top attacks. Compared to the rest of the technology services they are in the top 50% in remediating vulnerabilities. If this continues Mid-Size Data Management Company will be vulnerable to personal customer and employee information being leaked.

C 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 performing at an average level which increases the probability of an event occurring. You are currently in the Bottom 40% of companies within your industry. To improve your performance, ensure your company and your personnel follow current patching policies and procedures soon.
- Over the past 90 days there has been multiple hosts that are using Unsupported Browsers. This is a greater risk of system failure, disruption of business continuity, and attackers may be able to use unpatched vulnerabilities to gain system access.

Recommendations

WhiteHawk Cyber Analysts analyzed the security rating and risk vector performance results and provide the below tailored solution options to prevent and mitigate online crime and fraud thereby improving your company's overall cybersecurity posture. We base the solution options presented here 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 Recommendations

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:

Recommended Focus Area 1:

Communications Encryption: Due to improper TLS/SSL certifications and configurations, its current rating is decreasing significantly putting Mid-Size Data Management Company is in the bottom 30% of all companies. The result of this poor grade is from utilizing insecure protocols such as TLSv1.0 and TSLv1.1 Lastly your company is using shorter keypairs, Diffie- Hellman primes less than 2048 bits are estimated to be breakable by adversaries with nation-state-level resources. If this behavior continues your company will increase the risk on its security posture making it easier for actors to access sensitive data.

Recommended Focus Area 2:

Application Security: Over the past 90 days there has been multiple hosts that are using Unsupported Browsers. This is a greater risk of system failure, disruption of business continuity, and attackers may be able to use unpatched vulnerabilities to gain system access.

Recommended Focus Area 3:

Email Security: Mid-Size Data Management Company is in the top 40% of all companies in the technology industry for email security, please focus on generating new key pairs 2048 bits or greater into your DKIM configuration in order to increase your email security amongst the top companies in your industry.

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 within the context to your company's current IT implementation processes and implementations.

WhiteHawk presents three solution options for your consideration.

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**.

BASIC BUNDLE

BALANCED BUNDLE

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.

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.**

ADVANCED BUNDLE

BASIC BUNDLE

Email Filter: Sophos - Sophos Email Protection

Sophos Email is a secure email gateway engineered to keep businesses safe from all email threats. It simply stops spam, phishing, malware and data loss and keeps your people productive. And if you want to consolidate protection it lets you control email security alongside endpoint, mobile, web, and wireless protection from Sophos Central's single interface.

Training: KnowBe4 - 1 Year - Security Awareness Training

Three real-world scenarios show you strategies and techniques hackers use to take control of your computer system. You'll learn about the seven areas of an email that can contain red flags that alert you to a possible attack. The Danger Zone exercise will let you apply what you've learned.

BALANCED BUNDLE

Encrypted Communication: Symantec - Symantec Desktop Email Encryption

Protect your data in email, whether in transit or at rest. Symantec Desktop Email Encryption provides an end-to-end email encryption solution that automatically encrypts and decrypts email directly between clients without the need to log into a third-party website. Email remains encrypted on internal mail servers or when email is outsourced to the cloud.

Backup: StorageCraft - ShadowProtect IT Edition V5.x Subscription- 1 Year

ShadowProtect IT Edition PRO is perfect for taking quick backups, manage many Exchange servers and need to recover email messages or mailboxes, often have eDiscovery searches you need to perform, and/or have large migration projects you need to tackle. If you want "set it and forget it" system protection, where you can schedule backups throughout the day, you'll want to use ShadowProtect Server or ShadowProtect Desktop. If you do not manage Exchange servers, you'll want to use ShadowProtect IT Edition.

Patch Management: Micro Focus Software Inc. - Micro Focus Software Inc

ZENworks Patch Management, 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.

ADVANCED BUNDLE

Traffic Analysis: Forcepoint - SUREVIEW Insider Threat Core

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.

Security Information and Event Management: Micro Focus Software Inc. - Sentinel Enterprise

Here's a security solution that isn't as complex as the problem. Sentinel® is a full-featured Security Information and Event Management (SIEM) solution that simplifies the deployment, management and day-to-day use of SIEM, readily adapts to dynamic enterprise environments and delivers the true "actionable intelligence" security professionals need to quickly understand their threat posture and prioritize response.

Threat Manager: Verodin - Security Implementation Platform (SIP)

SIP instruments customer IT environments to test the effectiveness of network, endpoint, email and cloud controls. SIP continuously executes tests and analyzes the results to proactively alert on drift from a known-good baseline and validate control configuration. SIP provides evidence demonstrating if a customer's controls are actually delivering the desired business outcomes.

Orchestration: D3 Security - D3 SOAR

D3 is the only truly full-lifecycle security orchestration, automation, and response platform on the market. D3 has all the orchestration capabilities you need for rapid detection and remediation of security threats, but while other solutions might stop there, D3 is just getting started, with case management, forensics, and analytics capabilities that empower you to truly address vulnerabilities, instead of just treating the symptoms.

About Us

WhiteHawk is working with several Fortune 500 companies across multiple industries to implement the 360 Cyber Risk Framework. This includes contracts with a US Top 10 Financial Institution, the US Federal Government, and a US Top 12 Defense Industrial Base company.

WhiteHawk Inc., is the first AI-driven online Cybersecurity Exchange, uniquely positioned to continually vet and assess risk focused technologies, methodologies, and solutions that are impactful, affordable, and scalable. Since 2016, WhiteHawk has architected and implemented Cyber Risk Management Frameworks at the U.S. federal department level and at Fortune 500 Companies. We also help companies to connect to content, solutions, and service providers through evolving our rich data and user experience. WhiteHawk is a cloud-based platform that delivers virtual consultations and Cyber Risk Profiles that immediately match small and midsize business customers to tailored solutions on demand. The platform enables customers to leverage their tailored Security Story to find affordable and impactful cyber tools, content, and relevant services. Through our algorithms and expertise, we help companies and organizations better understand how to improve and stay ahead of today’s cyber threats. The Platform enables companies to fill their needs on an ongoing basis with demonstrated savings in time and cost.

In addition to hundreds of cybersecurity services and solutions available through the WhiteHawk Market Place and Cyber Consulting, we work with best-in-class partners to offer the following Reports:

— **Cyber Risk Profile Report**: Through a consultation with a Cyber Analyst, obtain recommendations for prioritizing products and services to addressing cyber security gaps.

— **Cyber Risk Scorecard Report**: Leverage security risk ratings to obtain recommendations for prioritizing products and services to addressing cyber security gaps.

— **Continuous Monitoring and Additional Services**: Through an annual subscription, obtain quarterly Cyber Risk Scorecards and consulting services. Includes continuous monitoring of cyber risks with historical context.

To learn more about WhiteHawk, our Tailorable Services, and Solution Partners, visit www.whitehawk.com and contact us. Cybersecurity and implementing actionable solutions do not need to be daunting; our Cyber Analysts can help you:

— Identify, understand, and prioritize risks

— Develop a customized Cyber Risk Action Plan and Maturity Roadmap

— Identify affordable solutions and services that align to your business objectives

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

WHITEHAWK®

Cyber Risk Scorecard

WhiteHawk CEC Inc

www.whitehawk.com