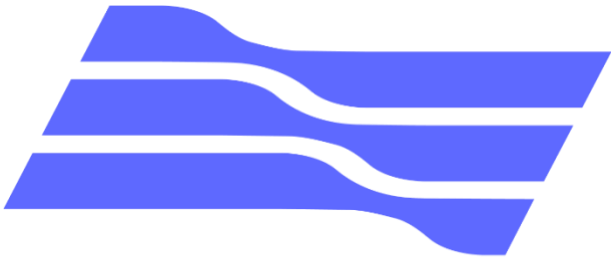

RHODIAN

RISK ASSESSMENT SAMPLE REPORT

SEPTEMBER 2024

Prepared For
ACME Corp

Prepared By
Rhodian Group
Aaron Wagner
Director, Cybersecurity Solutions

CONTENTS

EXECUTIVE SUMMARY

ACME Corp (AC) is a unified network of specialists with a corporate headquarters in New York, NY. During the period of October 24th, 2023, through January 3rd, 2024, Rhodian Group ("Rhodian") performed a Cybersecurity Risk Assessment on AC's Information Technology ("IT") systems. Overall, the assessment found that AC has implemented some IT security measures. However, Rhodian did identify a few high and medium priority security risk items during the assessment that should be addressed by management as soon as possible.

Overall, the majority of AC's operations are completed via SaaS applications and acceptable security controls are in place. It is worth noting that this environment and the completed workbook demonstrate a great level of understanding and implementing security practices.

The majority of items found in this risk assessment stem from the lack of documented policies and procedures around an accepted industry framework. Without an acceptable framework as a guide critical policies and procedures can be missed. While AC is a relatively new organization, and security is currently being prioritized, this lack of documentation can result in control misconfiguration or inconsistencies as the organization grows and scales.

Further investment in expanding the new information security policy will be beneficial in mitigating some of these risks and ensuring AC's cybersecurity program continues to mature. Rhodian did not identify any evidence this deal should not proceed.

ASSESSMENT DETAILS

PURPOSE

The goal of this Cybersecurity Risk Assessment was to identify critical systems, data, and existing controls in an effort to identify any threats and vulnerabilities related to the AC's IT assets, electronic protected health information ("ePHI") and related business procedures and provide recommendations on how to manage the identified risks via the appropriate administrative, physical, and technical safeguards. Rhodian Cybersecurity used industry recognized risk assessment methodologies including NIST guidance and proprietary methods.

SCOPE

The scope of the Cybersecurity Risk Assessment included data integrity protection and security, network security, physical security, and logical security (such as IT policies, IT security awareness, and maintenance) of the Company's IT assets.

Any outcome of our services is limited to a point-in-time assessment of the environment. Rhodian Cybersecurity does not constitute any form of representation, warranty, or guarantee that the systems tested are 100% secure from attack. Although a risk assessment is a key exercise in a cybersecurity program, its purpose is to identify areas of risk, not reduce areas of risk.

PERSONNEL

AC USA	Rhodian
John Doe VP, Information Technology johndoe@acmecorp.com	Aaron Wagner Director, Cybersecurity Solutions awagner@rhodiancybersecurity.com

ASSESSMENT METHODOLOGIES

The following methods were used to perform the Cybersecurity Risk Assessment.

Method	Description
Cybersecurity Risk Assessment Approach	Rhodian used a customized self-assessment questionnaire derived from the National Institute of Standards and Technology (NIST) SP 800-26, SP 800-53 Rev. 4, SP 800-53A Rev. 4 and FIPS 200.
IT Systems Assessment	Rhodian used screenshots and screen-sharing sessions to assess the current IT system configurations.
Resource Interviews	Rhodian conducted interviews with relevant staff to obtain and validate provided information.
Documentation Review	Rhodian reviewed the Company's security policies, system documentation, network diagrams, operations manuals, IT vendor services agreements and training materials.
Physical Security Review	The physical security portion of the assessment was handled remotely via policy review and resource interviews. No on-site analysis was performed.

RISK CALCULATION METHODOLOGY

The following categories were used to classify risk severity.

Risk Rating Scale	
CRITICAL	The finding represents a known risk to the confidentiality, integrity, and availability of sensitive data and/or business operations and should be addressed immediately.
HIGH	The finding represents a significant risk to the confidentiality, integrity, and availability of sensitive data and/or business operations and should be addressed immediately.
MEDIUM	The finding represents a moderate risk to the confidentiality, integrity, and availability of sensitive data and/or business operations and should be addressed in the IT roadmap.
LOW	Minimal risk of system or data compromise. Remediation should be balanced against business needs and compensating controls.

ASSESSMENT ANALYSIS

STAFF

AC employs 100 employees and 8 contractors to provide resources and support for revolution services. All employees have the ability to work remotely.

IT operations and HIPAA compliance are overseen by John Doe, VP of Information Technology. Jane Smith provides MSP support as needed and several IT support staff are available on a contractor basis.

AC conducts employee reference checks and background checks upon hire. Additionally, access is provided during the onboarding process by HR creating a ticket with user and access level required. An onboarding and offboarding inventory is in place. All employees are provided with a handbook that addresses the acceptable use of devices and computer security. An Information Privacy and Security policy is also provided to employees and contractors.

FACILITY SECURITY IT INFRASTRUCTURE

AC operates out of one corporate office in the state of Endor located at:

Table 1-1: Facility Access and IT Infrastructure Summary

Site	Access Type	Intrusion Alarm	Security Cameras	On-Premises Server	Firewall	Wi-Fi Access Points
Endor	Key	Yes	No	No	Yes	2

The office in Endor acts as the main office although employees may operate out of additional locations. As these locations are in charge of their own IT security, their security processes are outside the scope of this risk assessment.

The Endor office is indicated to have an intrusion alarm although no security cameras are in place in this leased location. The office is accessed by a physical key to unlock doors by five individuals. ID badges for employees are indicated to be a work in progress.

Visitors do not sign in although access to electronic information is protected with locked doors. AC stated that no facility walkthroughs are performed regularly.

IT INFRASTRUCTURE

The main office does not contain an on-premises server as all applications in use are third party cloud software. Servers and databases are hosted in an Azure environment. The main office does have a firewall in place and Wi-Fi access is provided through two access points. The firewall is managed by the internet service provider and access is controlled through a preshared key. It is unknown how often this key rotates and there is no formal policy in place.

ACCOUNT AND WORKSTATION SECURITY

According to the asset report provided, AC has approximately 70 workstations in use. Operating systems range from Windows 10 and 11 professional or enterprise editions. However, one system is indicated to be operating Windows 11 home premium edition.

AC's workstations are configured through Azure Active Directory to provide a username and password to log into workstations and there are no shared accounts in use. There are currently no idle lockout controls in place and failed login lockout is set at the default setting. All workstations are encrypted using BitLocker and devices may be remote wiped if stolen by initiating a script if they show back up online.

AC's password policy consists of three of the four complexities enabled and requires a minimum of 8 characters. MFA through Microsoft is also in place. Password recovery is achieved through the Microsoft process or by creating a helpdesk ticket. Administrative passwords are stored and managed using Bitwarden password management software.

Endpoint protections is administered through Carbon Black and device inventory is achieved using Ninja One.

Two personal devices are indicated to access company data and although Geofencing is in place for North America no other protections are in place for SaaS systems.

AC does not have a formal change management process in place.

APPLICATION AND DATA SECURITY

AC uses Microsoft Office 365 for corporate email accounts for management with MFA enabled. Mimecast is used for additional spam filtering and email encryption. OneDrive is utilized for online storage and access is determined by IT and Department leaders.

Files containing ePHI/PII used by AC are primarily stored within SaaS applications hosted by third party vendors. AC uses the third-party software below to support PHI/PII storage and operations. MFA and appropriate encryption standards are indicated to be in place for all systems containing ePHI and PHI. However, there is currently no formal policy for review of security settings and no data retention policies are in place.

- Exponent HR
- SQL Databases
- Snowflake for EDW

Only Monday.com, which is used for project management, was indicated to be lacking MFA.

RECORD RETENTION

No documentation was provided to Rhodian regarding retention of records. AC stated there are currently no policies in place.

IT DISASTER RECOVERY

AC indicated no formal incident response plan is currently in place although one is in the process of development. No documentation regarding disaster recovery, business continuity, or emergency evacuation was provided to Rhodian for review.

AC does not have a formal backup policy in place but MSP360 and Azure are backup up. However, no testing of disaster recovery plans is currently done.

ASSET DECOMMISSIONING

As a relatively new organization no electronic assets have been decommissioned and there is no procedure in place for this. Shred bins are utilized in the main office for any sensitive paperwork.

SECURITY AWARENESS AND EDUCATION

Mimecast is utilized for security awareness training and phishing emulation testing is conducted on a frequent basis. However, no HIPAA specific training is currently conducted although Mimecast does have these trainings available and AC is looking to roll this out in the near term.

COMPLIANCE AND AUDIT

AC is subject to HIPAA compliance and reporting and responding to security incidents is the responsibility of HIPAA Compliance Officer, John Doe.

Access permissions and software license and usage are reviewed on a biannual basis. An information security policy has just been completed and is planned to be reviewed annually. However, it is unclear if an industry accepted framework was utilized for this purpose as there are many gaps in documented policy.

AC does not currently conduct periodic vulnerability scanning or penetration testing of their environment.

The AC compliance team tracks incidents including security events using Ethicspoint software. A previous incident involving malware on a user's computer was identified and contained using Carbon Black. The computer was taken out of service and reimaged.

As part of this assessment an external and internal vulnerability scan was performed against the provided IP scope. Those findings are included in the vulnerability scan summaries provided separately from this report.

FINDINGS

The following risks were identified during the Cybersecurity Risk Assessment. The findings are prioritized based on risk severity, from most to least severe.

#	Severity	Finding	Description	Recommendations
1	CRITICAL	Windows Home Premium indicated to be in use	Most devices are running current Windows 10 or 11 Pro or Enterprise grade operating systems. However, one workstation is indicated to be running Windows 11 Home Premium. This version does not support Bitlocker drive encryption and Windows Information Protection (WIP) capabilities.	Upgrade this device to a pro or enterprise license to allow for more control or implement a more robust BYOD policy with minimum required security standards.
2	CRITICAL	Personal workstations used to access company resources	While becoming more common place in the remote work environment personal workstation devices, including Windows or Macintosh OS, do not offer the same level of security control and accountability as corporate managed devices. Instead, accountability is on the device owner to manage security and updates. This significantly increases the risk of endpoint compromise. Malware and endpoint compromise to gather credentials presents a known security risk to organizations using cloud-based resources.	Require company managed workstations to be used to access any company resources. -OR- Establish a clearly communicated BYOD policy that requires employees to utilize enterprise grade endpoint protection and updated OS.
3	CRITICAL	Synology DiskStation Manager is at end-of-life	It was indicated in the vulnerability scan that the Synology DiskStation Manager (DSM) version on the remote host has reached its End of Life (EOL) and is no longer receiving security updates from the vendor.	Update the DSM version to the most recently supported version as soon as possible to mitigate these risks. Additionally, back up all data before performing any upgrades.

4	**CRITICAL**	Netatalk 3.1.12 Arbitrary Code Execution	It was indicated in the vulnerability scan that Netatalk is vulnerable to an unauthenticated code execution exploit. Attackers can exploit this vulnerability an allow them to achieve arbitrary code execution on the target system.	Although the host is shielded behind a secure network, consider updating Netatalk to the latest version as soon as possible. This version includes patches and fixes for the Arbitrary Code Execution vulnerability.
5	**HIGH**	No HIPAA training currently in place	While Mimecast is used for security awareness and phishing training there is no HIPAA training currently done. This is indicated to be supported by Mimecast with intentions to roll out in the near future.	Utilize Mimecast to also provide HIPAA specific training during the onboarding process and on an annual basis for all employees.
6	**HIGH**	No MFA on Monday.com	Monday.com is indicated to be lacking MFA authentication. While there is no ePHI in this application it is indicated to include sensitive business critical data.	Enable MFA on Monday.com and ensure MFA on all SaaS solutions.
7	**HIGH**	No idle screen lockout and default failed login attempt settings	Workstation idle lockout and failed login monitoring are critical security controls in line with HIPAA and other compliance frameworks. While default settings for failed login attempts is a start, workstation settings should be further configured.	Enable idle lockout time of 15minutes for all workstations and ensure lockout of at least ten minutes after three failed login attempts.
8	**HIGH**	No vulnerability scanning, or penetration testing conducted.	Routine scanning for vulnerabilities and annual testing of the IT environment is critical to identifying misconfigurations, missing updates, and vulnerabilities that may be overlooked.	Perform vulnerability scanning of external and internal environment on a routine basis. Consider performing a penetration test of the internal, external, and wireless environments.

9	**HIGH**	Limited policies and procedures regarding IT	While a basic information security policy was provided this document leaves many gaps in addressing security concerns. This includes: • No formal change management process in place • No documented retention policy • No formal Incident response plan and no testing of disaster recovery process • No formal backup policy • No electronic assets decommissioning procedures • No Vendor Management Program in place	Create a centrally documented security program based around NIST or another industry framework to create standards for IT security, improve accountability, and reduce security risks. Review annually to ensure compliance and assign an individual responsible for maintenance of these documents.
10	**MEDIUM**	No walkthroughs performed regularly	Walkthroughs of physical locations are not performed on a regular basis. These are a critical step in identifying security issues and ensuring policies and procedures are followed.	Perform routine walkthroughs at the main office physical site to identify security violations.
11	**MEDIUM**	Badge identification currently in development	Identification badges are not currently worn although a process to do so was indicated to be in the works.	Proper identification of staff is critical to security and controlling access to facilities. Identification badges should be worn at each facility.
12	**MEDIUM**	No security cameras	While intrusion alarms are in place security cameras are not currently in use.	Consider installing a security camera system in cooperation with the office leasing agency, especially the entrances and exits of rooms that house sensitive data or critical IT assets. In addition to discouraging theft and vandalism, it can serve as a useful tool in security forensics should a break in occur.

13	LOW	Physical keys used for building access	Physical keys may be duplicated without approval, lost, or not returned by a terminated employee.	Consider installing RFI or PIN based access to buildings that can be provisioned by a remote computer. These systems can eliminate the identified risks and also maintain building access records.
14	LOW	No visitor sign in sheet	No visitor sign in sheet is utilized. While the office is indicated to be small this is a critical procedure to follow for liability purposes and to inventory those that come and go that are not part of the organization.	Create a process for visitor sign in and escort visitors through all controlled areas.

Rhodian Cybersecurity provides cybersecurity services to businesses nationwide. Over the past decade, our staff has supported hundreds of clients across diverse industries. As your trusted security advisor, we provide valuable insight to prevent attacks and can respond immediately to cybersecurity events. Utilizing a real-world approach, we combine information security best practices, human intelligence, and our vast experience to ensure your business is protected against the ever-evolving threat landscape. Our proven approach and experience has enabled us to become the preferred vendor for IT providers, MSPs, and various other organizations.

Rhodian Cybersecurity is HIPAA compliant and understands the needs of businesses striving to meet compliance for different industries, States, and Federal regulations.

CERTIFICATIONS AND ASSOCIATIONS

Rhodian is committed to supporting the information security community by being involved in industry events, organizations, and associations. Rhodian Cybersecurity staff maintain industry-recognized certifications and constantly pursue cutting-edge training.

- CompTIA Security+
- PNPT – Practical Network Penetration Tester
- CMMC-AB Registered Practitioner
- OSCP – Offsec Certified Professional
- CRTO – Certified Red Team Operator
- CRTP – Certified Red Team Professional
- CISM – Certified Information Security Manager

Rhodian and its staff are proud members and partners of the following associations:

- Applied Systems / Applied Client Network
- NetVU Gold Partner
- Vertafore Orange Partner
- Association for Independent Insurance Agents (Big “I”)
- Agents Council for Technology
- Catalyit Premium Solution Provider
- Fortified preferred vendor
- LIBRA preferred vendor
- SecureRisk preferred vendor