RHODIAN

RISK ASSESSMENT SUMMARY REPORT

Prepared For

ACME | John Doe | 555-555-5555 | client@acme.com

Contents

PROJECT DETAILS

Rhodian performed a Risk Assessment for Company to support their identification of key areas of risk within their IT Infrastructure. The assessment was performed during May-June 2021 with the objective of identifying critical systems, sensitive data, and protections in place to determine potential areas of risk.

Project Details

ACME	Rhodian
Project Sponsor John Doe 555-555-555 client@acme.com	**Project Lead** Aaron Wagner, Security + 513-532-9493 awagner@rhodian.com

Limitations

Any outcome of our services is limited to a point-in-time assessment of the environment. Rhodian 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.

Risk Acceptance

As outlined in NIST Special Publication 800-39 (Managing Information Security Risk), organizations may choose to accept cybersecurity risks. Acceptance of risk is tied to the success and achievement of business mission objectives, where mitigation of risk may unreasonably distract and disruptthe continued success and achievement of business objectives. Risk tolerance may also be acceptable when sufficient controls have been implemented to adequately reduce likelihood and impact of an attack.

EXECUTIVE SUMMARY

During May-June 2021, Rhodian performed a risk assessment for Company. The goal of this assessment was to identify critical systems, data, and existing controls in an effort to determine potential cybersecurity risks. Rhodian used industry recognized risk assessment methodologies including NIST guidance and proprietary methods.

High Risk System	
High-risk systems typically process, store, and transmit sensitive data. They are usually critical to the functions of the business, and a successful attack on these systems would have severe consequences. A lack of implemented cybersecurity controls may contribute to the increased likelihood of an attack.	
Local Routers, network switches, firewalls, modems ConvergeOne (Citrix Workspace App) Personal Email Systems	Zywave Agency Revolution Fuse Personal versions Microsoft Office 365

Medium Risk System	
Medium-risk systems may process, store, and transmit sensitive data. While the data may be sensitive, the systems are not mission critical, and a successful attack would not be detrimental to the business. Mediumrisk systems may contain missing cybersecurity controls; however, missing controls are limited and do not significantly increase the security of the system.	
Local desktop computers Mobile devices Employee personal computers	Dropbox Roboform OneHub

Low Risk System	
Low-risk systems do not process, store, or transmit sensitive information. The systems are still key to the business's success; however, the business could still function if the system is attacked or unavailable. Low risk systems may also be highly protected with advanced cybersecurity controls that include protection, detection, and response capabilities.	
Flash Drives/External Hard drive Voxo Phone Systems CSpire Phone Systems, Website	Payroll Website (Admin Access) Payroll Website (Individual Access)

KEY TAKEAWAYS & RECOMMENDATIONS

Rhodian was able to identify several key takeaways that were consistent among systems and the entirety of the cybersecurity program. The following is a list of key takeaways that should be remediated to reduce both the likelihood and impact of a successful cybersecurity attack. Generally speaking, the risk level of a system does not necessarily mean there are deficient cybersecurity controls – it is possible for a fully hardened and secure system to be high-risk due to the impact it has on business operations.

- An established cybersecurity program including documented policies and procedures mapped to an industry best practice framework is not currently in place. This results in a lack of overall implemented cybersecurity controls to protect the confidentiality, integrity, and availability of information systems across all offices. Implementing recommended cybersecurity protections and documenting these efforts in a centrally managed and standardized security program will significantly reduce the risk to IT systems managed and utilized by Company A. Company A is currently working with Rhodian to implement these risk reducing programs.

- Company A relies heavily on the use of the ConvergeOne Citrix desktop application to protect nonpublic information but lacks proper configuration of workstations and other controls in line with cybersecurity best practices. This includes lack of multifactor authentication, group accounts, and missing endpoint protection on some devices. This results in a lack of defense in depth to prevent security incidents and increases the overall risk of systems containing sensitive information. The differences in security configurations between branches could allow compromise at the most poorly secured location to propagate through the rest of the organization.

- Company A utilizes third-party vendors to support key business areas. Through these relationships, Company A has shared significant client data in the form of PII, potentially ePHI, proprietary data, financial information, and business-critical information. These relationships have not been assessed using due diligence practices outlined in NIST Special Publication 800-39 (Managing Information Security Risk)regarding trust modeling. Without centralized documentation such as a security program plan, this process may not have been followed adequately.

- Company A has experienced a security incident within the last three years. A previous compromise without documented lessons learned and corrective controls enabled significantly increases the likelihood of another security incident.

Rhodian recommends reviewing the Risk Assessment Workbook, provided separately from this report, which contains specific details regarding implemented and missing cybersecurity controls. Where gaps are identified, list these gaps and associated tasks for remediation within your plan of action and milestones (POA&M). As you address deficiencies create written policies and procedures to ensure the company follows due diligence and due care requirements.

SYSTEM SPECIFIC RESULTS

HIGH RISK SYSTEMS

Local Routers, Network Switches, Firewalls, Modems	
High Risk System	
System Purpose	Connect to the internet
Likelihood Determination	- Processes highly sensitive data - Presence of high number of vulnerabilities - Lack of specific cybersecurity protections - Overall cybersecurity protections lacking - Lack of incident response plan - Lack of continuous monitoring - Externally facing 3 rd party system
Impact Determination	- System security level is critical - System processes highly sensitive data - Impacts to Confidentiality are high - Impacts to Integrity are high - Impacts to Availability are high - A breach of the system may lead to a loss of customer trust - A breach of the system may result in breach notification requirements

Local Routers, Network Switches, Firewalls, Modems	
High Risk System	
System Purpose	Uses Citrix Workspace app to provide user desktops. Managed by third party vendor. Installed Agency Management System (client database)
Likelihood Determination	- Processes highly sensitive data - Lack of specific cybersecurity protections - Overall cybersecurity protections lacking - Lack of incident response plan - Lack of continuous monitoring - Externally facing 3 rd party system
Impact Determination	- System security level is critical - System processes highly sensitive data - Impacts to Confidentiality are high - Impacts to Integrity are high - Impacts to Availability are high - A breach of the system may lead to a loss of customer trust - A breach of the system may result in breach notification requirements

Local Routers, Network Switches, Firewalls, Modems	
High Risk System	
System Purpose	Email
Likelihood Determination	- Processes highly sensitive data - Lack of specific cybersecurity protections - Overall cybersecurity protections lacking - Lack of incident response plan - Lack of continuous monitoring - Externally facing 3rd party system
Impact Determination	- System security level is high - System processes highly sensitive data - Impacts to Confidentiality are high - Impacts to Integrity are high - Impacts to Availability are high - A breach of the system may lead to a loss of customer trust - A breach of the system may result in breach notification requirements

Agency Revolution Fuse	
High Risk System	
System Purpose	Email marketing
Likelihood Determination	- Processes highly sensitive data - Lack of specific cybersecurity protections - Overall cybersecurity protections lacking - Lack of incident response plan - Lack of continuous monitoring - Externally facing 3 rd party system
Impact Determination	- System security level is high - System processes highly sensitive data - Impacts to Confidentiality are high - Impacts to Integrity are high - Impacts to Availability are high - A breach of the system may lead to a loss of customer trust - A breach of the system may result in breach notification requirements

Zywave	
High Risk System	
System Purpose	Client email marketing
Likelihood Determination	- Processes highly sensitive data - Lack of specific cybersecurity protections - Overall cybersecurity protections lacking - Lack of incident response plan - Lack of continuous monitoring - Externally facing 3 rd party system
Impact Determination	- System security level is high - System processes highly sensitive data - Impacts to Confidentiality are high - Impacts to Integrity are high - Impacts to Availability are high - A breach of the system may lead to a loss of customer trust - A breach of the system may result in breach notification requirements

MEDIUM RISK SYSTEMS

Local Desktop Computers	
Medium Risk System	
System Purpose	Carrier websites, downloading client documents before attaching ConvergeOne, stored passwords in browsers
Likelihood Determination	- Processes highly sensitive data or medium sensitivity data - Lack of specific system cybersecurity protections - Overall cybersecurity protections lacking or medium gaps in overall cybersecurity protections - Lack of incident response plan or weak incident response plan - Lack of continuous monitoring or weak continuous monitoring efforts
Impact Determination	- System security level is medium - System processes medium sensitive data - Impacts to Confidentiality are low - Impacts to Integrity are low - Impacts to Availability are low - A breach of the system may lead to a loss of customer trust - A breach of the system may result in breach notification requirements

Mobile Devices	
Medium Risk System	
System Purpose	Email
Likelihood Determination	- Processes medium sensitivity data - Overall cybersecurity protections lacking or medium gaps in overall cybersecurity protections - Lack of incident response plan or weak incident response plan - Lack of continuous monitoring or weak continuous monitoring efforts - Externally facing 3 rd party system
Impact Determination	- System security level is medium - System processes medium sensitive data - Impacts to Confidentiality are medium - Impacts to Integrity are medium - Impacts to Availability are low - A breach of the system may lead to a loss of customer trust - A breach of the system may result in breach notification requirementsv

Employee Personal Computers	
Medium Risk System	
System Purpose	Document Storage System
Likelihood Determination	- Processes highly sensitive data sensitivity data - Lack of specific system cybersecurity protections - Overall cybersecurity protections lacking or medium gaps in overall cybersecurity protections - Lack of incident response plan or weak incident response plan - Lack of continuous monitoring or weak continuous monitoring efforts
Impact Determination	- System security level is high - System processes medium sensitive data - Impacts to Confidentiality are medium - Impacts to Integrity are medium - Impacts to Availability are medium - A breach of the system may lead to a loss of customer trust - A breach of the system may result in breach notification requirements

Dropbox	
Medium Risk System	
System Purpose	Document Storage System
Likelihood Determination	- Processes medium sensitivity data - Overall cybersecurity protections lacking or medium gaps in overall cybersecurity protections - Lack of incident response plan or weak incident response plan - Lack of continuous monitoring or weak continuous monitoring efforts - Externally facing 3 rd party system
Impact Determination	- System security level is low - System processes medium sensitive data - Impacts to Confidentiality are medium - Impacts to Integrity are low - Impacts to Availability are low - A breach of the system may lead to a loss of customer trust - A breach of the system may result in breach notification requirements

Roboform	
Medium Risk System	
System Purpose	Password Keeper
Likelihood Determination	- Processes highly sensitive data - Lack of specific system cybersecurity protections - Overall cybersecurity protections lacking or medium gaps in overall cybersecurity protections - Lack of incident response plan or weak incident response plan - Lack of continuous monitoring or weak continuous monitoring efforts - Externally facing 3rd party system
Impact Determination	- System security level is critical - System processes highly sensitive data - Impacts to Confidentiality are high - Impacts to Integrity are high - Impacts to Availability are medium - A breach of the system may lead to a loss of customer trust - A breach of the system may result in breach notification requirements

OneHub	
Medium Risk System	
System Purpose	Document Storage System
Likelihood Determination	- Processes highly sensitive data - Lack of specific system cybersecurity protections - Overall cybersecurity protections lacking or medium gaps in overall cybersecurity protections - Lack of incident response plan or weak incident response plan - Lack of continuous monitoring or weak continuous monitoring efforts - Externally facing 3rd party system
Impact Determination	- System security level is high - System processes highly sensitive data - Impacts to Confidentiality are medium - Impacts to Integrity are medium - Impacts to Availability are low - A breach of the system may lead to a loss of customer trust - A breach of the system may result in breach notification requirements

MEDIUM RISK SYSTEMS

Local Desktop Computers	
Lwo Risk System	
System Purpose	Client Documents
Likelihood Determination	- Processes medium sensitivity data - Some overall cybersecurity protections lacking or medium gaps in overall cybersecurity protections
Impact Determination	- System security level is low - System processes medium sensitivity data - Impacts to Confidentiality are medium - Impacts to Integrity are low - Impacts to Availability are lowv

Voxo Phone Systems/ CSpire Phone Systems	
Lwo Risk System	
System Purpose	Phones
Likelihood Determination	- Processes low sensitivity data - Externally facing 3rd party system
Impact Determination	- System security level is low - System processes low sensitivity data - Impacts to Confidentiality are low - Impacts to Integrity are low - Impacts to Availability are low

SouthGroupGulfCoast.com/SouthGroup.net	
Lwo Risk System	
System Purpose	Websites
Likelihood Determination	- Processes low sensitivity data - Externally facing 3rd party system
Impact Determination	- System security level is low - System processes low sensitivity data - Impacts to Confidentiality are low - Impacts to Integrity are low - Impacts to Availability are low

Payroll Website (Individual/Admin)	
Lwo Risk System	
System Purpose	Payroll
Likelihood Determination	- Processes low sensitivity data - Externally facing 3rd party system
Impact Determination	- System security level is medium - System processes low sensitivity data - Impacts to Confidentiality are high - Impacts to Integrity are low - Impacts to Availability are low

RHODIAN

Based in Colorado, Rhodian 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.

CERTIFICATIONS AND ASSOCIATIONS

All Rhodian staff maintain industry-recognized certifications from SANS, Offensive Security, and (ISC)² and constantly pursue cutting-edge training.

- GPEN - GIAC Penetration Tester
- OSWP - Offensive Security Wireless Professional
- OSCP - Offensive Security Certified Professional

Our company is committed to supporting the information security community by being involved in industry events and organizations. Rhodian and its staff are proud members of the following associations:

- ISSA | Denver Chapter
- Longmont Chamber of Commerce
- Colorado Technology Association
- Independent Insurance Agencies of Texas
- (ISC)²
- Professional Independent Insurance Agents of Colorado (PIIAC)
- Agency Council for Technology
- GIAC Advisory Board