HARNESS PROJECTS

Client Final Report

Cyber Risk Assessment

[redacted]

V 1.0

December 2024

Designed to deliver the final project outcome information about an organization's cyber risks.

Table of Contents

1.0 [redacted] Cyber Risk Assessment Report

1.1 Introduction

This report provides a comprehensive analysis of [redacted] cyber risk environment. It aims to identify potential cybersecurity threats, assess current vulnerabilities, and recommend strengthening the company's cyber defense mechanisms. The assessment is essential in ensuring that [redacted] remains resilient against the evolving landscape of cyber threats. By thoroughly evaluating the company's systems, policies, and procedures, this report aims to aid in crafting a strategic approach to mitigate identified risks effectively.

2.0 Executive Summary

The cyber risk assessment has identified several critical and high-level risks that could substantially affect [redacted] operations and data security. Key concerns include significant software vulnerabilities, hardware security deficiencies, and human factors that heighten potential cyber threats. The table below outlines the critical and high-priority risks requiring immediate action to safeguard business operations and maintain security.

Risk ID	**Risk Description**	**Likelihood**	**Consequence**	**Rating**
R1	Phishing Attacks	Likely	Major	High
R2	Ransomware Attacks	Likely	Extreme	Critical
R3	Insider data theft	Unlikely	Major	Moderate
R4	Password Controls	Likely	Major	Moderate

3.0 Risk Assessment

3.1 Risk Assessment Background

This section offers an in-depth overview of the organization's risk assessment process, outlining the 11-week assessment period and the methodologies utilized. These included thorough system analysis and employee interviews designed to comprehensively assess the organization's overall exposure to cyber risks.

IT Infrastructure and Software Overview

[redacted] IT infrastructure comprises a mix of on-premises and cloud-based solutions to support various business functions. The core components of the infrastructure include:

- Servers: Virtual servers hosting critical business applications and databases.
- Network Equipment: Local internet provider routers, firewalls, and other networking devices ensure connectivity and security.
- End-User Devices: Employees use desktops, laptops, and mobile devices.
- Cloud Services: Utilized for several business applications' storage, backup, and hosting.

The primary software applications in use include:

- Operating Systems: Various versions of Windows Server environments for end-user devices.
- Business Applications: Google Drive, Stripe, Slack, Google Analytics, Gmail, Zendesk, Zoom, QuickBooks, Superhuman, and MalCare.
- Security Software: Antivirus programs, intrusion detection/prevention systems (IDS/IPS), and encryption tools.

3.2 Threat Landscape

Cyber Attacks

[redacted] is vulnerable to various risks, including phishing attacks, ransomware, and human errors, due to permitting access to computers on personal networks without visibility into whether employees use the equipment for individual activities. Additional threats include software vulnerabilities, natural disasters, and theft.

Regulatory Compliance

[redacted] wants to follow GDPR (General Data Protection Regulation). GDPR has set global data privacy and security standards, influencing similar legislation worldwide, such as the California Consumer Privacy Act (CCPA) in the United States.

3.3 Vulnerability Assessment

Asset Identification

Asset ID	Asset Description	Owner	Location
A1	HR Database, Employee Personal Information, and Payroll	CEO	Cloud-Based Storage
A2	Hardware (Laptops, Printers, Scanners, Cellphones, etc.)	Everyone	Remote
A3	Employee Access Controls	CEO	Cloud Provider
A4	Business Website	CEO	Cloud-Based Storage
A5	Customer Support, Surveys	CEO & Operations MGR	Cloud-Based Storage

Software Vulnerabilities

Software	Vulnerability	Severity
Operating Systems	Unpatched exploits	High
Applications	Unencrypted Data	Medium

Hardware Vulnerabilities

Hardware	Vulnerability	Severity
Printers, Scanners, Thumb drives, External Hard drives, etc.	Outdated Firmware	High
Laptops	Outdated Hardware	Low
Cell Phones	Outdated Firmware	Low

Human Factors

This section examines the human factors contributing to cybersecurity risks, presented in a table to clearly outline key elements, associated vulnerabilities, and their severity. It evaluates various human-related risks, including deficiencies in training, policy non-compliance, and insufficient access controls. Recommendations are prioritized based on the severity of each vulnerability to ensure timely mitigation of critical issues. [redacted] faces significant risks in areas such as access control weaknesses, poor password management, undefined roles and responsibilities, lack of cybersecurity training, and insider neglect during remote work.

Factor	Vulnerability	Severity
Training	Lack of cyber awareness	High
Policies	Non-compliance	Medium
Access Controls	Weak Passwords	High
Access Controls	Shared Passwords	High

3.4 Risk Observations

Risk ID	Risk Description	Associated Asset(s)	Consequence (Impact, Insignificant, Minor, Moderate, Major, Extreme)	Likelihood (Almost Certain, Likely, possible, unlikely, Rare)	Risk Rating (based on Consequence and Likelihood)
R1	Unauthorized Access	Laptops, All Databases	Major	Likely	High
R2	Data breach in Customer Support Portal	Customer Support Portal	Major	Unlikely	Medium
R3	Data breach from outside network	All Databases	Moderate	Possible	Medium
R4	Compliance Regulations	The Business	Minor	Rare	Low
R5	Human Treat	Databases	Moderate	Possible	Medium
R6	Phishing Attacks	Laptops, All Databases	Major	Almost Certain	High
R7	Malware, Ransomware	All Databases	Major	Likely	High
R8	Loss or Damage to Assets	Software & Hardware	Minor	Possible	Low
R9	Unknown Vulnerabilities	Infrastructure and Website	Major	Almost Certain	High

3.5 Existing Controls Assessment

Unfortunately, the only controls that exist are the ones provided by third-party services such as Google, QuickBooks, Slack, and Stripe.

3.6 Action Plan (Risk Treatments)

Action Plan ID	**Risk ID(s)**	**Treatment Description**	**Objective**	**Priority**	**Responsible Person/Team**
AP1	Implement MFA and a Non-Password Sharing Policy	R1	High	Limit the use of human error and unauthorized access.	Executive Management
AP2	Increase the frequency of security audits for the Customer Support Portal.	R2	Medium	Ensure that customers' information is secure and no malicious activity occurs.	Operations Team
AP3	Implement a VPN Network for remote access	R3	Medium	All employees are on a secure network when during company operations.	Executive Management
AP4	Implement standardized applications for business use	R4	Low	Employees are all using the same applications	Executive Management

AP5	Access Control Plan	R5	Medium	Limit controls on access. Create a policy for those who have access to specific systems.	Executive Management
AP6	Cybersecurity Protection Training Policy	R6	High	Everyone needs consistent training on cybersecurity trends.	IT Department & Executive Management
AP7	Monitoring Policy	R7	Low	Monitor activity consistently to catch security breaches.	IT Department
AP8	Terms & Conditions Policy	R4	Low	Keep the Terms & Conditions policy up to date and implement changes annually.	Executive Management
AP9	Disaster Recovery Plan	R8	Low	Implement a recovery plan for emergencies.	Executive Management and the entire staff.
AP10	Bug Bounty Program or Penetration Testing	R9	Medium	Scan for vulnerabilities consistently to reduce threats.	IT Department

3.7 Conclusion

The assessment underscores significant software and hardware vulnerability risks compounded by human factors. [redacted] can reduce these risks and strengthen its cybersecurity posture by adopting the recommended controls. As cyber threats continue to evolve, maintaining vigilance and adapting cybersecurity measures are essential to safeguarding the integrity and privacy of both company and customer data. By investing in robust risk management strategies, [redacted] addresses current vulnerabilities and proactively positions itself to tackle future security challenges.

Appendix: Vulnerability Risk Evaluation Methodology

The Vulnerability Risk Evaluation Methodology outlines how [redacted] assesses and prioritizes vulnerabilities in its IT infrastructure based on the potential impact and likelihood of exploitation. This methodology is designed to ensure consistent and comprehensive evaluation and to facilitate informed decision-making for remediation efforts.

Risk Evaluation Process

1. **Identification**: Detect vulnerabilities through automated scanning tools, manual testing, and third-party reports.
2. **Classification**: Classify vulnerabilities based on their type and location within the infrastructure—software, hardware, or process.
3. **Assessment**: Evaluate each vulnerability for its potential impact on confidentiality, integrity, and availability of systems and data, and determine the likelihood of exploitation.
4. **Prioritization**: Prioritize vulnerabilities for remediation based on the assessed risk level using the Risk Matrix provided.
5. **Remediation**: Develop and implement strategies to mitigate or eliminate high and critical risks. Monitor and reassess medium and low risks regularly.
6. **Documentation**: Maintain comprehensive records of identified vulnerabilities, assessments, decisions made, and outcomes of remediation efforts.

Risk Matrix

The Risk Matrix uses two main criteria: The likelihood of exploitation and the Consequence of exploitation. These criteria are defined as follows:

- **Likelihood**:
  - **Almost Certain**: Expected to occur in most circumstances
  - **Likely**: Will probably occur in most circumstances
  - **Possible**: Might occur at some time
  - **Unlikely**: Could occur at some time
  - **Rare**: May only occur in exceptional circumstances
- **Consequence**:
  - **Insignificant**: No impact on operations or individuals
  - **Minor**: Minor impact, easily remedied

- **Moderate**: Causes a noticeable level of disruption and may incur costs
- **Major**: Significant impact, substantial intervention required
- **Extreme**: Very costly, severe impact on operations or safety

Risk Evaluation Table

Likelihood	**Consequence**				
	Insignificant	**Minor**	**Moderate**	**Major**	**Extreme**
Almost Certain	**Low**	**Moderate**	**High**	**Critical**	**Critical**
Likely	**Low**	Moderate	High	High	**Critical**
Possible	**Low**	Moderate	Moderate	High	**High**
Unlikely	**Low**	Low	Moderate	Moderate	**High**
Rare	**Low**	Low	Low	Moderate	**Moderate**