Scratchpad Template

Cyber Risk Assessment Project

Designed to capture data and insights during the project work, which will not necessarily be included in the final client report.

Table of Contents

General Information

1. Date: 11/25/2024
2. Cyber assessor (Student) Name: Christian Stevens
3. Client company name: [redacted]
4. Assessor's objectives: Provide general security policies for current and potential growth.

Client Interview - Scratchpad Report Template

Designed to capture detailed information about an organization's cyber risks.

Organization Information

1. Organization Name: [redacted]
2. Contact Person: [redacted]

Stakeholders

[redacted]

Scheduling and Logistics

1. Start Date: 10/02/2024
2. End Date: 12/10/2024
3. Expected Duration: 9-11 Weeks
4. Outside Working Hours: Anytime

Introduction and Executive Summary

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.

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

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 assess the organization's overall exposure to cyber risks comprehensively.

Asset Identification

List all critical assets within the organization.

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

Questions and Information Gathering

Question ID	**Topic**	**Question**	**Date Asked**	**Information Gathered**
Q1	Client Assets	Do you currently have a way of tracking all company assets, such as an MDM?	11/12/2024	No.
Q2	Client Assets	Do you require a hardware/firmware update on employee computers?	11/12/2024	No, but it is recommended but not monitored.

Q3	Client Assets	Is specific software required on employee computers?	11/12/2024	No.
Q4	Vulnerability Identification	Is there any vulnerability management tool currently in place? If so, what software is in use?	11/12/2024	Google Business
Q5	Vulnerability Identification	How often do you conduct vulnerability assessments, and do you think this frequency is adequate?	11/12/2024	They do not conduct assessments.
Q6	Preventative Measures	How do you monitor network traffic for suspicious activity, and how effective is this monitoring?	11/12/2024	Website tracking is the only thing being monitored.
Q7	Preventative Measures	What process is followed to secure remote connections to your network?	11/12/2024	None.
Q8	Email Filtering	Which email filtering tools are currently used to manage incoming and outgoing mail?	11/12/2024	Google Workspace, Gmail, and Superhuman on phones.
Q10	Email Filtering	Is there a process in place for employees to report suspected phishing attempts?	11/12/2024	Not officially.
Q11	Network & Wi-Fi Security	Are there any specific compliance requirements employees need to adhere to?	11/12/2024	None.
Q12	Network & Wi-Fi Security	Are any specific tools or software used to monitor and manage network security?	11/12/2024	None.
Q13	Network & Wi-Fi Security	How often is security training provided to employees regarding network and Wi-Fi	11/12/2024	Training does not exist now.

		security?		
Q14	Risk Log Management	Are there specific log sources that are critical for monitoring or troubleshooting?	11/12/2024	There are server logs and AI conversation logs that are manually checked.
Q15	Risk Log Management	What are the most critical systems and applications that need logging?	11/12/2024	Quality control for user experience and site stability.
Q16	Risk Log Management	Who should have access to the logs, and what permissions do they need?	11/12/2024	The CEO and IT personnel have access.
Q17	Endpoint Protection and Device Security	What devices are in use (e.g., laptops, desktops, mobile devices, IoT) and need protection?	11/12/2024	Cellphones and laptops.
Q18	Endpoint Protection and Device Security	How do we currently handle device authorization and deauthorization?	11/12/2024	No procedure is in place. But they would have the account locked down if they saw something suspicious.
Q19	Endpoint Protection and Device Security	Are there privacy considerations for employees, primarily if they use their devices for personal and work purposes?	11/12/2024	No. It is not clear if employees use devices for personal use, but it can be assumed that they do.
Q20	IDS/IPS	Are there specific network segments that are a higher priority for monitoring or protection?	11/12/2024	Not concerned for users but want them protected from Courtroom5.
Q21	IDS/IPS	How important is it to have real-time versus periodic threat detection?	11/12/2024	It is preferred.
Q22	IDS/IPS	Are there specific events or thresholds that should trigger alerts?	11/12/2024	Unexpected and/or unauthorized uploads.

Q23	Authentication & Passwords	Should certain users or roles (e.g., administrators) follow stricter authentication protocols?	11/12/2024	Yes.
Q24	Identity & Access Management	What is the process for reviewing and updating roles or permissions?	11/12/2024	None.
Q25	Identity & Access Management	How should new user accounts be created, and who is responsible for provisioning?	11/12/2024	The CEO performs these tasks based on need.
Q26	Identity & Access Management	Should administrators receive specialized training for managing roles, permissions, and IAM configurations?	11/12/2024	Yes.
Q27	Authentication & Passwords	Are there specific policies for password reuse, history, or uniqueness?	11/12/2024	None, but they agree that they must have a policy in place.
Q28	Authentication & Passwords	What should the process be for account recovery if users forget their passwords?	11/12/2024	Currently it is controlled by the CEO or site provider.
Q29	Privileged Access Management	What types of privileged accounts currently exist within the organization?	11/12/2024	None.
Q30	Privileged Access Management	Who is responsible for approving access requests for privileged accounts?	11/12/2024	The CEO.
Q31	Privileged Access Management	How do stakeholders perceive the balance between security and operational efficiency in PAM?	11/12/2024	Unfortunately passwords are being shared with the CEO having all access.

Q32	Penetration Testing	When was the last penetration test conducted?	11/12/2024	The last test was conducted in December 2023

Software Vulnerabilities

List and describe significant software vulnerabilities identified during the risk assessment. This should include vulnerabilities discovered through automated tools and those uncovered during manual testing or interview workshops. Explain the potential impact of these vulnerabilities and any existing controls or lack thereof.

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

Hardware Vulnerabilities

This section presents a comprehensive inventory of hardware vulnerabilities in a tabular format, offering a clear overview of the nature and severity of each issue. The table highlights vital hardware components, including printers, workstations, and network devices, along with their identified vulnerabilities and corresponding severity ratings. This structured layout quickly identifies critical areas requiring urgent attention, supporting efficient prioritization and action planning.

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

Threat Landscape

[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 personal 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.

Risk Observations

Identify and describe potential risks to the assets listed above.

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

---

Existing Controls

Document current controls in place to mitigate identified risks.

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

Additional Notes and Observations

Capture any additional information, observations, or insights relevant to the risk assessment.

- Note 1: The company needs a base for standardized policies.
- Note 2: Employee training on phishing awareness is lacking.
- Note 3: Defined roles and responsibilities need to be determined.
- Note 4: Software and other programs must be consistent among all employees.
- Note 5: Access controls are not in place and are critical to security.
- Note 6: Vulnerabilities are unknown due to a lack of testing.
- Note 7: Lack of a Disaster Recovery Plan could hurt operations.

Action Plan Ideas

Brainstorm potential action plans to address identified risks and improve existing controls.

Action Plan ID	Action Plan Description	Associated Risk(s)	Priority	Objective	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 and/or Penetration Testing	R9	Medium	Scan for vulnerabilities on a consistent basis to reduce threats.	IT Department