LUMBERJACK LOGISTICS COMPANY

RISK MANAGEMENT PLAN

Version *1.0*

05/14/2024

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	*Zachary Vivian*	*05/14/2024*	*Dr. Bassam Zahran*	*05/14/2024*	Initial Risk Management Plan

TABLE OF CONTENTS

1 INTRODUCTION

1.1 PURPOSE OF THE RISK MANAGEMENT PLAN

A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project's objectives. Risk Management is the process of identifying, assessing, responding to, monitoring, and reporting risks. This Risk Management Plan defines how risks associated with the Lumberjack Logistics Company project will be identified, analyzed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the lifecycle of the project and provides templates and practices for recording and prioritizing risks. The Risk Management Plan is created by the project manager in the Planning Phase of the Lumberjack Logistics Company Unified Process and is monitored and updated throughout the project. The intended audience of this document is the project team, project sponsor and management.

Lumberjack Logistics Company is a well-established company within the logistics and retail industry, so this risk management plan is made for an in-house risk management team. We feel that given the substantial operations the company has, a significant investment in IT and a hardened security infrastructure is necessary to support business activities and save the company from potential revenue loss due to security breaches.

(Estimated) Total Annual Company Revenue: **$750,000,000**

2 RISK MANAGEMENT PROCEDURE

2.1 PROCESS

The project manager working with the project team and project sponsors will ensure that risks are actively identified, analyzed, and managed throughout the life of the project. Risks will be identified as early as possible in the project so as to minimize their impact. The steps for accomplishing this are outlined in the following sections. The project manager will serve as the Risk Manager for this project.

A. Risk Identification:
    a. The purpose of identifying risks is to analyze potential threats to the company, typically with historical data review/previously logged incidents.

B. Risk Assessment:
    a. This is to qualitatively access probability/impact for each risk using risk management, and then quantitatively assess potential financial impact.

C. Risk Response Planning:
    a. Knowing our identified threats and potential impacts, we can choose to avoid (eliminate the risk entirely), mitigate (reduce probability/impact of risk), accept (acknowledge the risk and prepare plans if it were to occur), or transfer (outsource the risk to a third party)

D. Risk Monitoring and Control:
    a. The job of the risk management team is to continuously monitor these risks and reassess statuses should an incident occur. This should be tracked in a risk management log for easy reference.

E. Risk Reporting:
   a. Typically, managing a risk log is important to communicate changes in risk to management and stakeholders promptly. We can also document our responses to these risks and their outcomes for lessons learned and future reference.

F. Tools and Practices:
   a. Finally, we suggest various tools and practices we can implement to track, manage, and respond to risks.

2.2 RISK IDENTIFICATION

Risk identification will involve the project team, appropriate stakeholders, and will include an evaluation of environmental factors, organizational culture and the project management plan including the project scope. Careful attention will be given to the project deliverables, assumptions, constraints, WBS, cost/effort estimates, resource plan, and other key project documents. A Risk Management Log will be generated and updated as needed and will be stored electronically in the project library located at <file location>.

1. Denial of Service

A denial-of-service attack is a cyber-attack where the attacker targets the availability aspect of cybersecurity. It does this by interrupting a host’s services from a network. One common version of this attack is the TCP SYN flood attack. In this attack the attacker takes advantage of the TCP three-way handshake, where the attacker sends the initial SYN packet, the victim server sends the SYN-ACK back, but the attacker does not respond with the final ACK packet, which will eventually cause the server to run out of resources. The easiest way to identify and mitigate this attack is to identify illegitimate traffic that is being used in the denial-of-service attack, and block that illegitimate traffic.

2. Business Email Compromission

A business email compromission is a type of phishing attack where an attacker impersonates a trusted figure in a corporation and requests sensitive information from another employee. The request for sensitive information may be in the form of a request to pay an urgent bill, asking for a phone number, or an expiring lease. There are a few simple ways to detect and prevent business email compromission. The easiest is to use a secure email solution, like Office 365, that automatically detects and will alert you of suspicious emails.

3. Ransomware

Ransomware is a type of malware that encrypts a victim’s data, and the attacker offers to decrypt the data if a ransom is paid. The easiest way to protect against ransomware is to perform frequent backups of your system, so you can just restore your system to the state saved on the backup. Another easy way to prevent ransomware is to make sure all applications and operating systems within the organization are up to date.

4. Malware

Malware is any malicious software that interferes with the normal functions of a computer. If a computer is infected with malware it may slow down, crash, serve many pop-ups, change your default search engine, send emails you didn’t write, or run out of battery quicker. To identify if you have malware download a trustworthy security software to scan your computer. Any flagged software should be deleted as soon as possible.

5. Cross-Site Scripting

Cross-site scripting is a form of cyber-attack where an attacker is able to inject scripts into web pages viewed by other users, and run that script on the other users. To identify if your application is vulnerable to cross-site scripting, you can simply use a web vulnerability scanner. These scanners can also detect SQL Injection attacks, command injection, path traversal, and insecure server configuration.

6. Phishing/Social Engineering

Phishing is a form of social engineering where the attack deceives their target to get them to reveal sensitive information or install malware. One common type of phishing attacks is email phishing. The attacker in email phishing use email to trick other individuals into giving away sensitive information. SMS phishing is another type of phishing that uses text messages to bait the victim into revealing sensitive information. The best way to prevent phishing attacks is to train employees how to identify these phishing emails and text messages, so they never even open the email. Employees should also never respond to phishing campaigns.

7. Insider Threats

An insider threat is the potential for an authorized user to use their access in the organization to harm the organization. Insider threats may be looking to commit espionage, terrorism, steal information, sabotage, or create loss of resources and capabilities. Insider threats can be difficult to defend against, as most cyber security systems focus on preventing damage from unauthorized attacks. Some anomalies to look for to identify an insider threat are; unusual network and system assessments, unexpected spikes in network traffic, requesting access to documents not required for one’s role, and using personal devices without approval. Some network indicators of an insider threat are; backdoors in the network, unapproved software downloads, and manually disabling security tools.

8. Sensitive Customer Data Theft

Sensitive customer data theft is usually due to a data breach. A data breach is a security incident where an attacker gains unauthorized access to sensitive information. One of the most effect methods to mitigate damage from a data breach is having an effective incident response plan, which includes a framework for detecting, containing, and eradicating cyberthreats.

9. Confidential Company Data Theft

Confidential company data is usually stolen in data breaches, similarly to customer data. Also similar to customer data, the most effective mitigation technique is keeping an effective incident response plan.

10. Employee Data Theft

Employee data theft is when an employee intentionally or unintentionally exposes company information. One of the most effective defense mechanisms for this is using the principle of least privilege. Giving employees the minimum amount of permissions needed will keep sensitive data in front of the least eyes possible.

11. Fake Webstores/Company Impersonation

Website spoofing is a scam where an attacker creates a website that closely resembles a trusted website, as well as its domain. This is done in order to trick customers, suppliers, or employees into using this website instead of the real one, and disclosing sensitive information, such as logins. To identify and prevent website spoofing, double check domains to make sure they are an exact match to what you expect.

12. Social Media Misinformation

Social media misinformation is misleading or false information that is spread through social media platforms. This includes fake news articles, misleading images or videos, conspiracy theories, or misinformation campaigns. Misinformation campaigns can damage a companies reputation. To mitigate misinformation campaigns encourage media literacy, fact-checking, and user reporting.

2.3 RISK ANALYSIS

All risks identified will be assessed to identify the range of possible project outcomes. Qualification will be used to determine which risks are the top risks to pursue and respond to and which risks can be ignored.

1. Denial of Service

There are many possible outcomes when it comes to denial-of-service attacks. One outcome is loss of revenue which happens due to our services being down since the business is not functioning normally. Reputational damage is another big outcome that is possible from denial of service as this will make the company look unreliable, which will also create lower customer satisfaction. Resources will also need to be used on a denial-of-service attack; the IT team will have to put resources into mitigating this attack, which will take away their valuable time and slow down other tasks.

2. Business Email Compromission

Potential outcomes from an attack like this such as financial loss, reputational damage, data loss, and many other outcomes. Attackers may trick employees into putting funds into fraudulent accounts, along with this they can get information about different employees and even more internal information from the company. A possible outcome from this attack would be a loss of data, attackers can potentially get sensitive data from this attack which can lead to even more security concerns.

3. Ransomware

Outcomes of ransomware can include data loss, revenue loss, and damage to reputation. Ransomware will encrypt data making it inaccessible until the ransom is paid, in some cases the data will be corrupted or destroyed once the attack is over. Like most other cyber-attacks, this leads to financial losses. This attack can be stressful for employees which can lead to a morale loss and employees will not perform their job at their upmost efficiency. Ransomware should not be paid because this will show the attacker that we comply with their attacks and make it more likely to happen again in the future.

4. Malware

Malware can delete or make files un accessible along with stealing the data in the process. It is not just the data that is at risk, but the entirety of the company's information systems can become infected. Malware can use system resources such as the CPU and memory which will slow down the performance. There are many types of malware, such as key loggers which capture what is being inputted from the keyboard to steal credentials to get access to other systems. Similar to other risks, there are outcomes with both financial and reputational loss.

5. Cross-Site Scripting

Attackers may use the attack to impersonate users and access their account, to steal their information and or perform different actions pretending to be the victim. Cross-site scripting can also be used to spread malware, and trick users into doing different unwanted actions. This attack can lead to financial and reputational loss, with the possibility of legal penalties.

6. Phishing/Social Engineering

Phishing and Social Engineering are some of the most common attacks; these attacks will manipulate the victim into showing sensitive information or performing certain actions. If successful, the attacker can take over accounts leading to unauthorized transactions. This attack can result in the attacker gaining employee access to the organization's data, which ultimately could lead to another attack such as ransomware or simply the unauthorized modification of data. This could lead to a loss of revenue due to having to fix damaged or lost data.

7. Insider Threats

Insider threats can come from an insider employee who is being negligent or someone who is trying to harm the company on purpose. Insider threats can lead to financial, reputational, and legal consequences depending on the severity of the insider threat. Most insider threats come from a disgruntled employee, which is why it's important to have proper training and policies in place—informing employees of possible implications of their actions. An insider looking to do harm may steal data or sabotage systems which can lead to even more problems, costing the company valuable time and resources.

8. Sensitive Customer Data Theft

Customer data theft will have many repercussions, especially reputational damage. When customer data gets stolen it will eventually be made public. This will lead to a negative view of the company's protection of their data, damaging their reputation. With the company in a negative light, we will lose customers which will then cause the company to lose money. Depending on the data stolen there may be regulatory penalties leading to significant fines being paid. Customer data theft would be a public relations nightmare and may lead to legal and court fees.

9. Confidential Company Data Theft

Company data is important and should be kept safe. If company data is not kept safe, it can lead to various things such as disrupted operations and financial/reputational losses. If some intellectual property or secrets are stolen the company has the potential to lose future announcements which may positively or negatively affect shareholders' view of the company. Company data is important and should be kept safe along with putting proper backups in place.

10. Employee Data Theft

It's important employees have proper security training as employee data theft is typically leaked through phishing which could be prevented with proper training. Depending on what kind of data is stolen the attacker can use it to steal identities/pretend to be an employee and modify or delete data. This creates problems for both the employee and the company. These credentials may allow the attacker to adventure even further into the systems of the company, this scenario could cost the company a significant amount of money just in investigating the issue at hand.

11. Fake Webstores/Company Impersonation

Fake webstores can cause lost potential revenue or reputational damage for the company. Customers will shop at these fake webstores selling mock versions of our product and the company will also be losing the potential revenue from customers meaning to shop at the legitimate site. It is also likely that these websites are getting customer data and employee data depending on the size of the operation. It is important that we take down impersonators as soon as possible to prevent a false view of the company from a customer standpoint and from spending their money not on our real product.

12. Social Media Misinformation

Social media has been huge and continues to grow rapidly, if misinformation gets put out it can be spread fast which would not be good for public relations. Fewer customers will lead to less revenue, we will also have to put more resources into PR to help salvage our reputation. It is also important to learn where the information started to make sure it is not part of an even bigger problem. Additionally, it is important for the company to have a social media personality to positively reflect the company and address any rumors/misinformation that may arise.

2.3.1 Qualitative Risk Analysis

The probability and impact of occurrence for each identified risk will be assessed by the project manager, with input from the project team using the following approach:

Probability

- High – Greater than *70%* probability of occurrence
- Medium – Between *30%* and *70%* probability of occurrence
- Low – Below *30%* probability of occurrence

Impact

- High – Risk that has the potential to greatly impact project cost, project schedule or performance
- Medium – Risk that has the potential to slightly impact project cost, project schedule or performance

- Low – Risk that has relatively little impact on cost, schedule or performance

Risks that fall within the RED and YELLOW zones will have risk response planning which may include both a risk mitigation and a risk contingency plan.

Impact	*HIGH*	**R7**	**R1**	**R3, R4, R8**
	MEDIUM	**R2**	**R5, R6, R9, R10**	**R11, R12**
	LOW			
		LOW	*MEDIUM*	*HIGH*
	Probability			

Risk List

Risk	Description	Risk Level
R1	Cybercrime—Denial of Service	HIGH
R2	Cybercrime—Business Email Compromise	LOW
R3	Cybercrime—Ransomware	HIGH
R4	Cybercrime—Malware	HIGH
R5	Cybercrime—Cross-Site Scripting	MEDIUM
R6	Cybercrime—Phishing/Social Engineering	MEDIUM
R7	Cybercrime—Insider Threats	LOW
R8	Data Theft—Sensitive Customer Data	EXTREME
R9	Data Theft—Company Confidential Data	MEDIUM
R10	Data Theft—Employee Data	LOW
R11	Online Brand Risk—Fake Webstores/Company Impersonation	HIGH
R12	Online Brand Risk—Social Media Misinformation	HIGH

2.3.2 Quantitative Risk Analysis

Analysis of risk events that have been prioritized using the qualitative risk analysis process and their effect on project activities will be estimated, a numerical rating applied to each risk based on this analysis, and then documented in this section of the risk management plan. The monetary impact is an estimate based off of potential revenue loss, reputation loss, and time it takes to fix the issue/bolster security to prevent it from happening again.

1. **Denial of Service**

Probability: **0.8 (High)**
Estimated Monetary Impact: **$1,000,000**
Risk Exposure (RE = P x I): **$800,000**

2. **Business Email Compromission**

Probability: **0.2 (Low)**
Estimated Monetary Impact: **$300,000**
Risk Exposure (RE = P x I): **$60,000**

3. **Ransomware**

Probability: **0.8 (High)**
Estimated Monetary Impact: **$2,000,000**
Risk Exposure (RE = P x I): **$1,600,000**

4. **Malware**

Probability: **0.8 (High)**
Estimated Monetary Impact: **$800,000**
Risk Exposure (RE = P x I): **$640,000**

5. **Cross-Site Scripting**

Probability: **0.5 (Medium)**
Estimated Monetary Impact: **$500,000**
Risk Exposure (RE = P x I): **$250,000**

6. **Phishing/Social Engineering**

Probability: **0.5 (Medium)**
Estimated Monetary Impact: **$750,000**
Risk Exposure (RE = P x I): **$375,000**

7. **Insider Threats**

Probability: **0.2 (Low)**
Estimated Monetary Impact: **$600,000**
Risk Exposure (RE = P x I): **$120,000**

8. **Sensitive Customer Data Theft**

Probability: **0.8 (High)**
Estimated Monetary Impact: **$4,000,000**
Risk Exposure (RE = P x I): **$3,200,000**

9. **Confidential Company Data Theft**

Probability: **0.5 (Medium)**
Estimated Monetary Impact: **$1,000,000**
Risk Exposure (RE = P x I): **$500,000**

10. **Employee Data Theft**

Probability: **0.2 (Low)**
Estimated Monetary Impact: **$200,000**
Risk Exposure (RE = P x I): **$40,000**

11. **Fake Webstores/Company Impersonation**

Probability: **0.8 (High)**
Estimated Monetary Impact: **$1,000,000**
Risk Exposure (RE = P x I): **$800,000**

12. Social Media Misinformation

Probability: **0.8 (High)**
Estimated Monetary Impact: **$500,000**
Risk Exposure (RE = P x I): **$400,000**

2.4 RISK RESPONSE PLANNING

Each major risk (those falling in the Red & Yellow zones) will be assigned to a project team member for monitoring purposes to ensure that the risk will not "fall through the cracks". For each major risk, one of the following approaches will be selected to address it:

- **Avoid** – eliminate the threat by eliminating the cause
- **Mitigate** – Identify ways to reduce the probability or the impact of the risk
- **Accept** – Nothing will be done
- **Transfer** – Make another party responsible for the risk (buy insurance, outsourcing, etc.)

For each risk that will be mitigated, the project team will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include prototyping, adding tasks to the project schedule, adding resources, etc. For each major risk that is to be mitigated or that is accepted, a course of action will be outlined for the event that the risk does materialize in order to minimize its impact.

1. Denial of Service

The best way to avoid denial of service attacks is by blocking traffic from malicious sources. This can be done by setting a rule on the network's firewall blocking IPs from sources known to be used in botnets.

2. Business Email Compromission

The best way to mitigate risks associated with business email compromission (BEC) is to train employees on recognizing BEC attacks, and what to do when they identify a BEC attack. Another method to mitigate effects from a BEC attack is implementing controls such as multi-factor authentication and VPNs to ensure users attempting to login to the network are who they say they are.

3. Ransomware

One of the best ways to avoid ransomware is to regularly update software. This will help ensure any known vulnerabilities will have the required patches to keep your data safe. Another way to avoid ransomware is using a secure email service. Most ransomware attacks are carried out through email phishing attacks. A secure email service will automatically block suspicious emails that could be phishing emails. A final way to avoid ransomware is implementing endpoint security such as anti-malware software. An anti-malware software can detect ransomware on a device and quarantine that device to prevent the ransomware from spreading.

4. Malware

A good way to avoid malware is by implementing controls to prevent employees from downloading software without approval. This will help keep employees from unintentionally downloading malware onto company machines. Another way to avoid malware is by installing anti-malware software that can check software downloads and scan machines for known malware.

5. Cross-Site Scripting

To mitigate cross-site scripting attacks, user input should be sanitized for HTML and JavaScript code. Another way to mitigate cross-site scripting attacks is to implement a web application firewall (WAF). Rules on the WAF can be created to block abnormal server requests, which can prevent cross-site scripting attacks.

6. Phishing/Social Engineering

In order to mitigate phishing attacks, employees should be trained to recognize phishing emails, and how to deal with them according to company policy. Another way to mitigate phishing attacks is to use a secure email service. Using an email service that automatically flags and blocks phishing emails is one of the best ways to mitigate phishing attacks.

7. Insider Threats

To mitigate insider threats the company should use the principle of least privilege in their access control system. This will keep sensitive data in front of the least number of people possible, and give insider threats the least amount of power possible. The company should also keep a protective and supportive culture that encourages employees to report suspicious behaviors in the company.

8. Sensitive Customer Data Theft

To avoid data theft the principle of least privilege should be used in access control systems. This will minimize the effects from any privileged accounts that are compromised. Companies should also strengthen endpoint security. Effective antivirus should be used to prevent malware from compromising sensitive data.

9. Confidential Company Data Theft

To avoid confidential company data theft from occurring, the same controls should be implemented as the ones to avoid sensitive customer data theft.

10. Employee Data Theft

To mitigate employee data theft companies should use the principle of least privilege in access control systems. A process to quickly revoke privileges after user termination should be implemented to prevent disgruntled former employees from stealing data. Another effective way to mitigate employee data theft is implementing auditing software with log collection to identify what resources are accessed by employees and create accountability.

11. Fake Webstores/Company Impersonation

To mitigate website spoofing we need to implement a solution that prevents spoofing attacks. To do so, we recommend the implementation of social media monitoring tools as well as a domain monitoring service tool to identify possible fake companies attempting to gain our customers and sell them fake products. After identifying these websites, we can take them down since we have the rights to our products and make sure our customers can find what they're looking for without having to sift through duplicate websites attempting to harvest their information in return for cheaper prices.

12. Social Media Misinformation

To mitigate social media misinformation companies should swiftly make public responses to misinformation campaigns. This will allow the company to get the correct information out to the public and maintain their reputation. Another way to mitigate social media misinformation is to encourage fact checking on social media sites. With a social media manager as well as some implemented tools, we can help stop the spread of misinformation.

2.5 RISK MONITORING, CONTROLLING, AND REPORTING

The level of risk on a project will be tracked, monitored and reported throughout the project lifecycle. A "Top 10 Risk List" will be maintained by the project team and will be reported as a component of the project status reporting process for this project. All project change requests will be analyzed for their possible impact to the project risks. Management will be notified of important changes to risk status as a component to the Executive Project Status Report.

For logging risks, all risks that have been identified will be recorded in a risk register that will include information about them—such as where the attack came from, what techniques they used, and how we defended against the risk/what we need to implement to prevent it in the future. This will include any current risks along with any new risks that show up, each new risk will be assessed for likelihood and impact and then the prioritization list will be updated as needed. Along with recording and assessing the risk, a plan must be developed to mitigate each new risk. Risk must also be continuously monitored to keep track of their status and make sure we aren't being impacted.

For reporting risks, the list of risks will be included in status reports that will be distributed to the project stakeholders along with mitigated plans so that the stakeholders have information that we are keeping track of new threats. If there are any significant changes to any of the risks, they will be reported to senior management officials to ensure they are aware of any ongoing developments. Not only this, but there should be regular meetings to discuss the status of risks and to review the effectiveness of the mitigation strategies.

Communication will play a big part as we need to make sure everyone is on the same page to prevent further problems, this will include updates when it comes to the monitoring, controlling, and reporting any current or new risks. Communication must be maintained in order to make sure that everyone understands the process and how it fits within the process.

3 TOOLS AND PRACTICES

A Risk Log will be maintained by the project manager and will be reviewed as a standing agenda item for project team meetings.

Security Tools & Protections	Recommended Software

Firewalls/Filters	Firewalls work by controlling incoming network traffic based off defined security rules. This means we have a barrier between our internal trusted network and untrusted external networks.	Palo Alto Next-Generation Firewall
Virtual Private Network	This allows employees to securely connect to the company's internal network over the internet. This encrypts all data transmitted between the user's device and the corporate network. VPN's help protect sensitive data, secure remote access, and ensure compliance with data protection regulations.	Palo Alto Networks GlobalProtect
Email Security Gateways/Email Filtering	Email security gateway and filtering solutions can protect email-based threats such as phishing, malware, and spam. This software scans incoming/outgoing emails to ensure the company's security.	Barracuda Email Security Gateway
Anti-Virus	Anti-virus software can detect, prevent, and remove malicious software from company computers. These provide real-time protection and frequent scanning.	Bitdefender Antivirus Plus
Endpoint Protection Platforms	Endpoint protection platforms provide security for endpoint devices like desktops, laptops, and mobile devices. As an extra layer of security, these combine aspects of anti-virus, firewall, and other tools.	CrowdStrike Falcon
Domain Monitoring Service	Domain monitoring services track and monitor domains related to the brand to detect and prevent domain-related threats such as hijacking and typo squatting.	DomainTools
Social Media Monitoring	Social media monitoring tools can track company mentions, comments, and other activities to help detect and respond to misinformation/malicious activities.	Brandwatch
Demilitarized Zone	A DMZ is a segment of the network that sits between the internal network and the external network. This adds another layer of security by isolating sensitive systems from direct exposure to the internet.	pfSense
Segmentation	Network segmentation involves dividing a network into small segments (ex. different	Cisco Meraki

	sections like corporate and retail networks) to improve security and performance. This limits the spread of malware and restricts access to sensitive data.	
Intrusion Detection System	IDS monitor network traffic for suspicious activities/potential threats. This detects and alerts system administrators for potential security breaches.	Snort
Data Loss Prevention	DLP solutions prevent sensitive data from being lost, misused, or accessed by unauthorized individuals. These monitor & control data transfers, ensuring data protection.	Forcepoint DLP
Password Policies	Password policies enforce rules for creating and managing passwords, ensuring they are strong and secure. These help prevent against unauthorized access, and make brute force attacks significantly more difficult.	LastPass Enterprise
Two Factor Authentication	2FA adds yet another layer of security by requiring a second form of identification (usually a text or email) before granting access to systems or data.	Duo Security
Access Control	Access control systems can manage who has access to resources and data. This ensures that only authorized individuals have access to sensitive information, minimizing the risk of lower-trust users from accessing this data.	Microsoft Azure Active Directory
Incident Reporting/Response	Incident reporting/response tools help the company detect, investigate, and respond to security incidents effectively and efficiently, limiting the impact of security breaches.	Splunk Phantom
Backup & Restore	Backup and data restoration solutions ensure that data is regularly backed up and can be restored in the event of data loss from hardware failure, ransomware, or other security incidents.	Acronis Cyber Backup
Data Encryption	Data encryption tools protect data by converting it into a secure format that can only be read by authorized users, ensuring data confidentiality and integrity.	BitLocker, FileVault

Input Validation	Input validation ensures data entered into applications is checked and sanitized to prevent security vulnerabilities such as SQL injection and cross-site scripting.	OWASP ZAP, BurpSuite
Logging/Analytics	Logging and analytics tools collect and analyze logs from various systems to detect security incidents, monitor system health, and ensure compliance.	Graylog
Security Assessments/Auditing	Regular security assessments and auditing evaluate the organization's security posture, identify potential vulnerabilities, and ensure compliance with security policies and regulations.	Nessus
Security Awareness	Security awareness tools educate all employees about security best practices, phishing, social engineering, and other threats in order to minimize the risk of human error.	KnowBe4
Security Training	Regular security training programs provide IT and security professionals with the in-depth knowledge and skills necessary to manage and protect and organization's IT infrastructure.	Infosec Institute

Infrastructure	
Total Users	In total, the company has 2500 users among corporate offices and retail stores.
Windows Machines	The company has 1000 Windows computers.
Mac Machines	The company has 200 Mac computers.
Active Directory Servers	The company has 2 primary, and 2 backup active directory servers for user authentication, policy management, and directory services.
File Servers	The company has 6 file servers for distributed file storage across all locations. This provides central storage for documents, files, and shared resources.
Application Servers	The company has 8 application servers to support business applications.

Database Servers	For database information, the company has 2 primary servers and 2 backup servers for storing and maintaining company databases.
Web Servers	The company has 2 servers for internal applications and 2 for external-facing services.
Backup Servers	With a total of 4 backup servers, 2 are on site and 2 are off-site for redundancy, ensuring disaster recovery and storing frequent backups.
Firewalls	The company has a total of 4 firewalls for network security, monitoring, and traffic filtering.
Switches	The company has 20 total switches for network connectivity and traffic management.
Routers	The company has a total of 6 routers (in the data centers) for routing traffic between different network segments.
Load Balancers	A total of 4 load balancers distributes incoming traffic across multiple servers to ensure high availability.
Wireless Access Points	100 total wireless access points (distributed among corporate offices and retail stores) to provide employees with wireless network access.
VPN Gateways	4 VPN gateways provide secure remote access to the network for employees working from home.
Disaster Recovery Sites	2 geographically separate disaster recovery sites ensure business continuity in case of a major incident such as a tornado.

Based on our suggestions for implementing various tools and techniques to help the company mitigate identified risks, the company will need to spend roughly **$2,362,000** per year to maintain security staff and licenses to the tools necessary to defend the company from cyber-attacks. Additionally, the up-front cost for all the necessary hardware for the company will cost roughly **$902,000**. *Note: These are rough estimates and many not 100% accurately reflect their real-life values, we simply put these here since they most likely would be involved in a complete Risk Management Plan.*

Security Tools: **$982,000/year**

Palo Alto Next-Generation Firewall: $10,000 per firewall = **$40,000**

Palo Alto Networks GlobalProtect (VPN): **$15,000**

Barracuda Email Security Gateway: **$5,000**

Bitdefender Antivirus Plus: $30 per device = **$36,000**

CrowdStrike Falcon (Endpoint Protection): $70 per device = **$84,000**

DomainTools (Domain Monitoring): **$25,000**

Brandwatch (Social Media Monitoring): **$15,000**

pfSense (DMZ): **$1,000**

Cisco Meraki (Segmentation): **$40,000**

Snort (IDS): **$10,000**

Forcepoint DLP: **$40,000**

LastPass Enterprise (Password Policies): $5 per user per month = **$150,000**

Duo Security (Two-Factor Authentication): $6 per user per month = **$180,000**

Microsoft Azure Active Directory (Access Control): $4 per user per month = **$120,000**

Splunk Phantom (Incident Reporting/Response): **$50,000**

Acronis Cyber Backup: **$60,000**

BitLocker/FileVault (Data Encryption): $5 per device = **$6,000**

OWASP ZAP/BurpSuite (Input Validation): **$10,000**

Graylog (Logging/Analytics): **$15,000**

Nessus (Security Assessments/Auditing): **$10,000**

KnowBe4 (Security Awareness): **$20,000**

Infosec Institute (Security Training): **$30,000**

IT Professionals Team: **$1,380,000/year**

(1) Chief Information Security Officer: **$200,000/year**

(3) Security Analysts: **$90,000/year each**

(2) Network Security Engineers: **$100,000/year each**

(3) Systems Administrators: **$80,000/year each**

(2) Incident Response Team: **$85,000/year each**

(5) IT Support Staff: **$60,000/year each**

Hardware: **$902,000** up front

Active Directory Servers: 4 servers (2 primary, 2 backup)

Estimated Cost: $10,000 per server

Total: **$40,000**

File Servers: 6 servers

Estimated Cost: $10,000 per server

Total: **$60,000**

Application Servers: 8 servers

Estimated Cost: $15,000 per server

Total: **$120,000**

Database Servers: 4 servers (2 primary, 2 backup)

Estimated Cost: $20,000 per server

Total: **$80,000**

Web Servers: 4 servers (2 internal, 2 external)

Estimated Cost: $10,000 per server

Total: **$40,000**

Backup Servers: 4 servers (2 on-site, 2 off-site)

Estimated Cost: $20,000 per server

Total: **$80,000**

Firewalls: 4 firewalls

Estimated Cost: $10,000 per firewall

Total: **$40,000**

Switches: 20 switches

Estimated Cost: $5,000 per switch

Total: **$100,000**

Routers: 6 routers

Estimated Cost: $7,000 per router

Total: **$42,000**

Load Balancers: 4 load balancers

Estimated Cost: $15,000 per load balancer

Total: **$60,000**

Wireless Access Points: 100 access points

Estimated Cost: $500 per access point

Total: **$50,000**

VPN Gateways: 4 gateways

Estimated Cost: $10,000 per gateway

Total: **$40,000**

Backup Storage:

Total: **$50,000**

Storage Area Network (SAN):

Total: **$100,000**

RISK MANAGEMENT PLAN APPROVAL

The undersigned acknowledge they have reviewed the **Risk Management Plan** for the ***Lumberjack Logistics Company*** project. Changes to this Risk Management Plan will be coordinated with and approved by the undersigned or their designated representatives.

Signature: Zachary Vivian Date: 05/14/2024

Print Name: Zachary Vivian

Title: Risk Management Author

Role: Created Risk Management Plan

Signature: Date: 05/14/2024

Print Name: [Name Here]

Title: Chief Information Security Officer

Role: Overseer of Information Security

Signature: Date: 05/14/2024

Print Name: [Name Here]

Title: Chief Technology Officer

Role: Overseer of Company's Technological Direction

Signature: Date: 05/14/2024

Print Name: [Name Here]

Title: Chief Executive Officer

Role: Makes Major Corporate Decisions Aligning with Company Goals

APPENDIX A: KEY TERMS

The following table provides definitions for terms relevant to the Risk Management Plan.

Term	Definition
Access Control	A method of managing access to information systems and data, ensuring only authorized users can access specific resources.
Anti-Virus	Software designed to detect, prevent, and remove malicious software from computers and networks.
Backup and Restore	Procedures and technologies used to create copies of data to protect against loss, and to restore data after loss or corruption.
Botnet	A network of infected computers controlled by an attacker to perform tasks such as sending spam or launching distributed denial-of-service (DDoS) attacks.
Cross-Site Scripting (XSS)	A security vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users.
Data Encryption	The process of converting data into a coded format to prevent unauthorized access.
Denial of Service (DoS)	An attack that aims to make a network service unavailable to its intended users by overwhelming it with traffic.
Domain Monitoring Service	Tools that track and monitor domains related to a brand to detect and prevent domain-related threats such as hijacking and typo-squatting.
Firewall	A network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
Intrusion Detection System (IDS)	Software or hardware designed to detect unauthorized access or anomalies within a network.
Key Logger	A type of malware that records keystrokes to capture sensitive information such as usernames and passwords.
Malware	Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems.
Multi-Factor Authentication (MFA)	A security system that requires more than one method of authentication from independent categories of credentials to verify a user's identity.
Phishing	A type of social engineering attack where attackers pose as legitimate entities to steal sensitive information through fraudulent emails, websites, or messages.

Ransomware	A type of malware that encrypts a victim's data, demanding a ransom to restore access.
Security Information and Event Management (SIEM)	Tools that provide real-time analysis of security alerts generated by applications and network hardware.
Sensitive Data	Information that must be protected due to its confidential nature, such as personal identifiable information (PII) or financial data.
Social Engineering	The use of psychological manipulation to trick individuals into divulging confidential information or performing actions that compromise security.
SQL Injection	A code injection technique that exploits a security vulnerability in an application's software by inserting malicious SQL statements into an entry field.
Virtual Private Network (VPN)	A technology that creates a secure and encrypted connection over a less secure network, such as the internet.
Vulnerability Assessment	The process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.
Web Application Firewall (WAF)	A security solution that protects web applications by filtering and monitoring HTTP traffic between a web application and the internet.
Zero-Day Exploit	A cyberattack that occurs on the same day a weakness is discovered in software before the developer has had a chance to create a fix.