Contents

Overview

This assignment will present a cybersecurity risk management strategy tailored to SolarWinds Corporation. The risk management strategy is divided into three categories.

Category 1 addresses asset evaluation by classifying SolarWinds' physical, digital, and human assets through CIA Triad and Business Impact Analysis to determine their criticality and sensitivity.

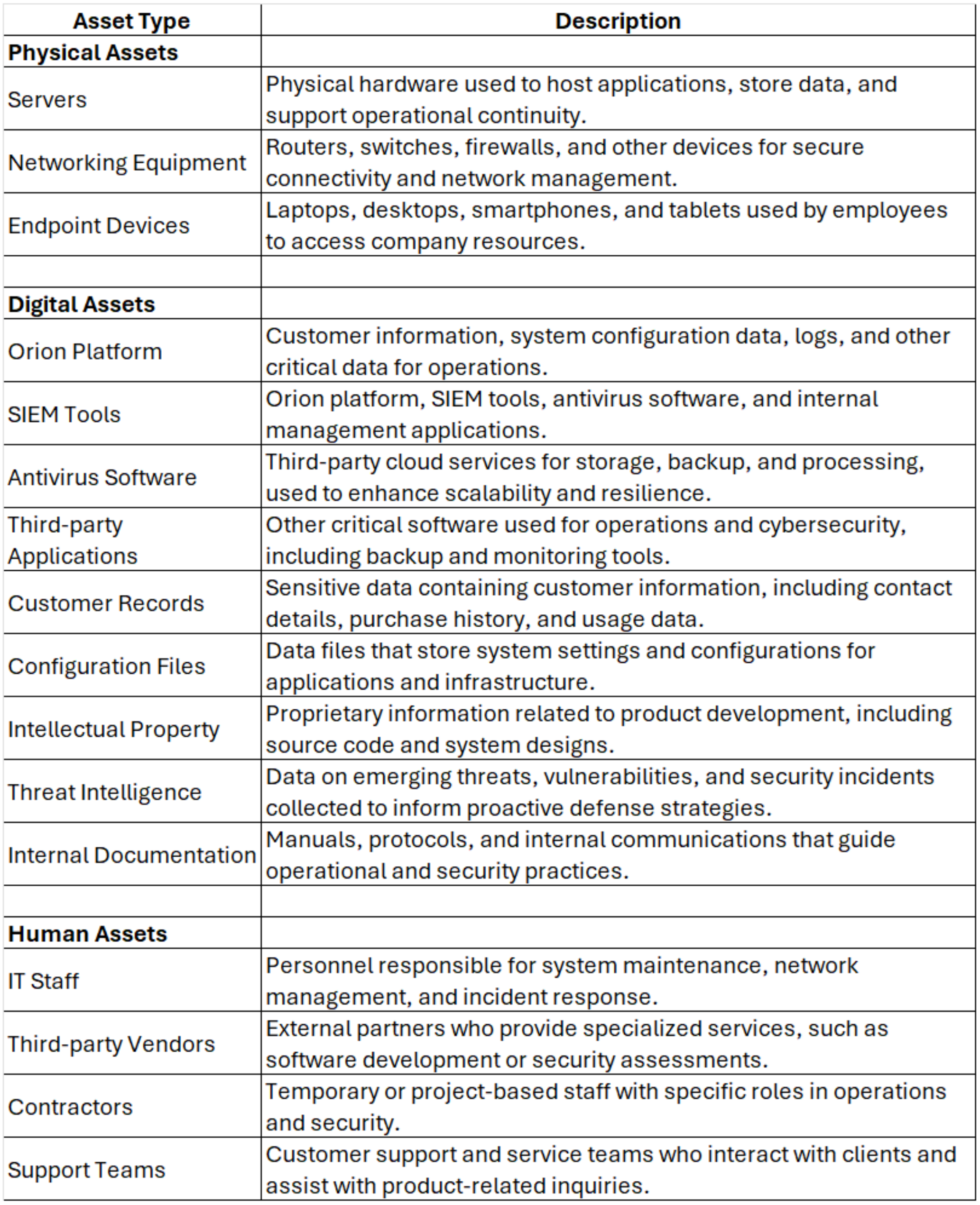
Category 2 focuses on evaluating and monitoring risks with qualitative and quantitative assessments, Key Risk Indicators (KRIs), and a structured periodic review to adapt to evolving threats.

Category 3 prioritizes cost-effective risk treatments, conducting a cost-benefit analysis, and implementing security controls with clear metrics to enhance SolarWinds' cybersecurity resilience.

Component 1: Asset Evaluation and Classification

1.1 Asset Inventory Creation:

A well-defined asset inventory is essential for understanding the types of resources SolarWinds relies on and how each contributes to its operational goals. This inventory includes physical, digital, and human assets, each playing a role in delivering services,

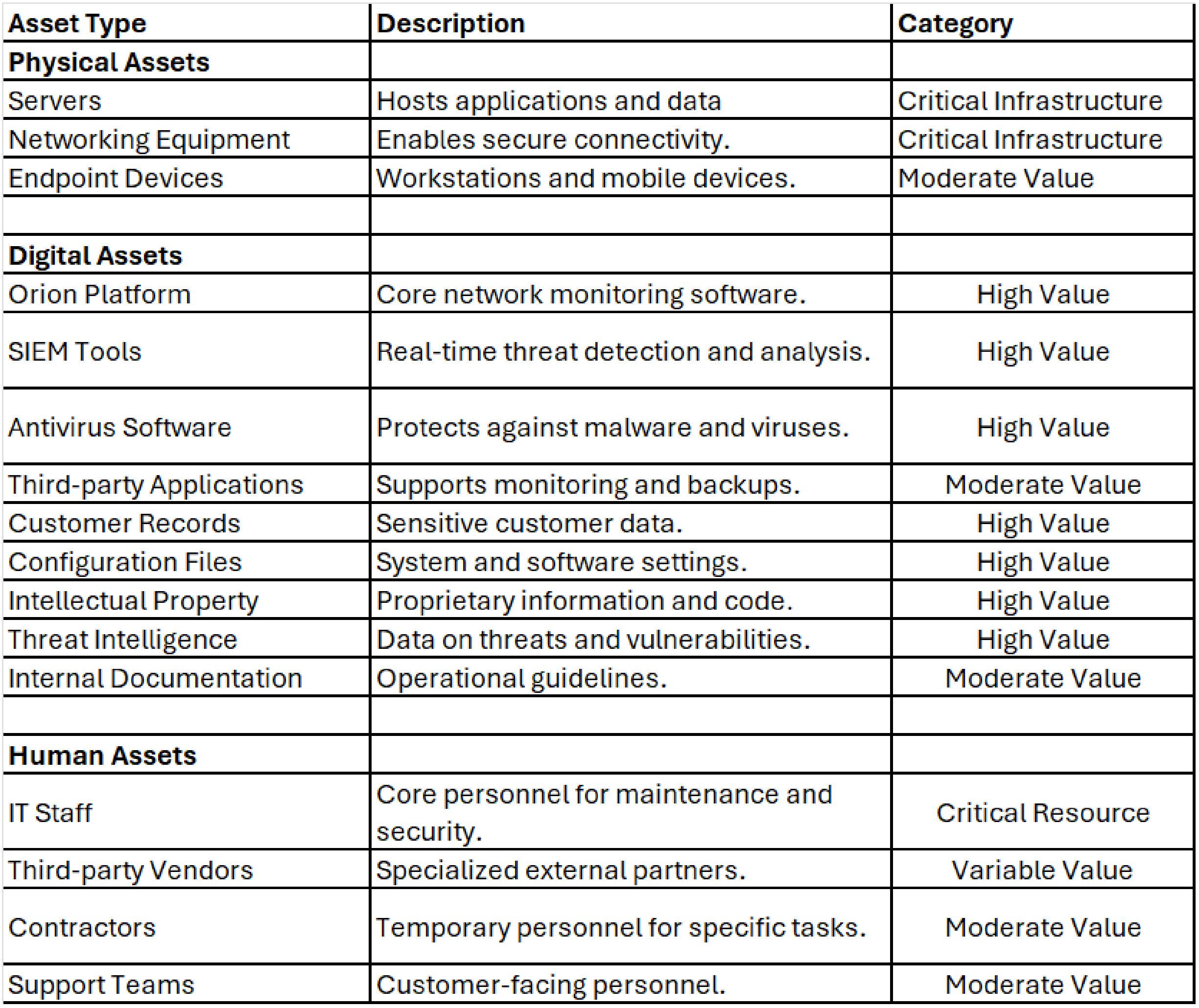


Asset Type	Description
Physical Assets	
Servers	Physical hardware used to host applications, store data, and support operational continuity.
Networking Equipment	Routers, switches, firewalls, and other devices for secure connectivity and network management.
Endpoint Devices	Laptops, desktops, smartphones, and tablets used by employees to access company resources.
Digital Assets	
Orion Platform	Customer information, system configuration data, logs, and other critical data for operations.
SIEM Tools	Orion platform, SIEM tools, antivirus software, and internal management applications.
Antivirus Software	Third-party cloud services for storage, backup, and processing, used to enhance scalability and resilience.
Third-party Applications	Other critical software used for operations and cybersecurity, including backup and monitoring tools.
Customer Records	Sensitive data containing customer information, including contact details, purchase history, and usage data.
Configuration Files	Data files that store system settings and configurations for applications and infrastructure.
Intellectual Property	Proprietary information related to product development, including source code and system designs.
Threat Intelligence	Data on emerging threats, vulnerabilities, and security incidents collected to inform proactive defense strategies.
Internal Documentation	Manuals, protocols, and internal communications that guide operational and security practices.
Human Assets	
IT Staff	Personnel responsible for system maintenance, network management, and incident response.
Third-party Vendors	External partners who provide specialized services, such as software development or security assessments.
Contractors	Temporary or project-based staff with specific roles in operations and security.
Support Teams	Customer support and service teams who interact with clients and assist with product-related inquiries.

securing customer data, and maintaining service availability (National Institute of Standards and Technology, 2018).

By categorizing assets into physical, digital, and human assets, SolarWinds can better assess their criticality in the risk management process and ensure that security measures align with each asset's function.

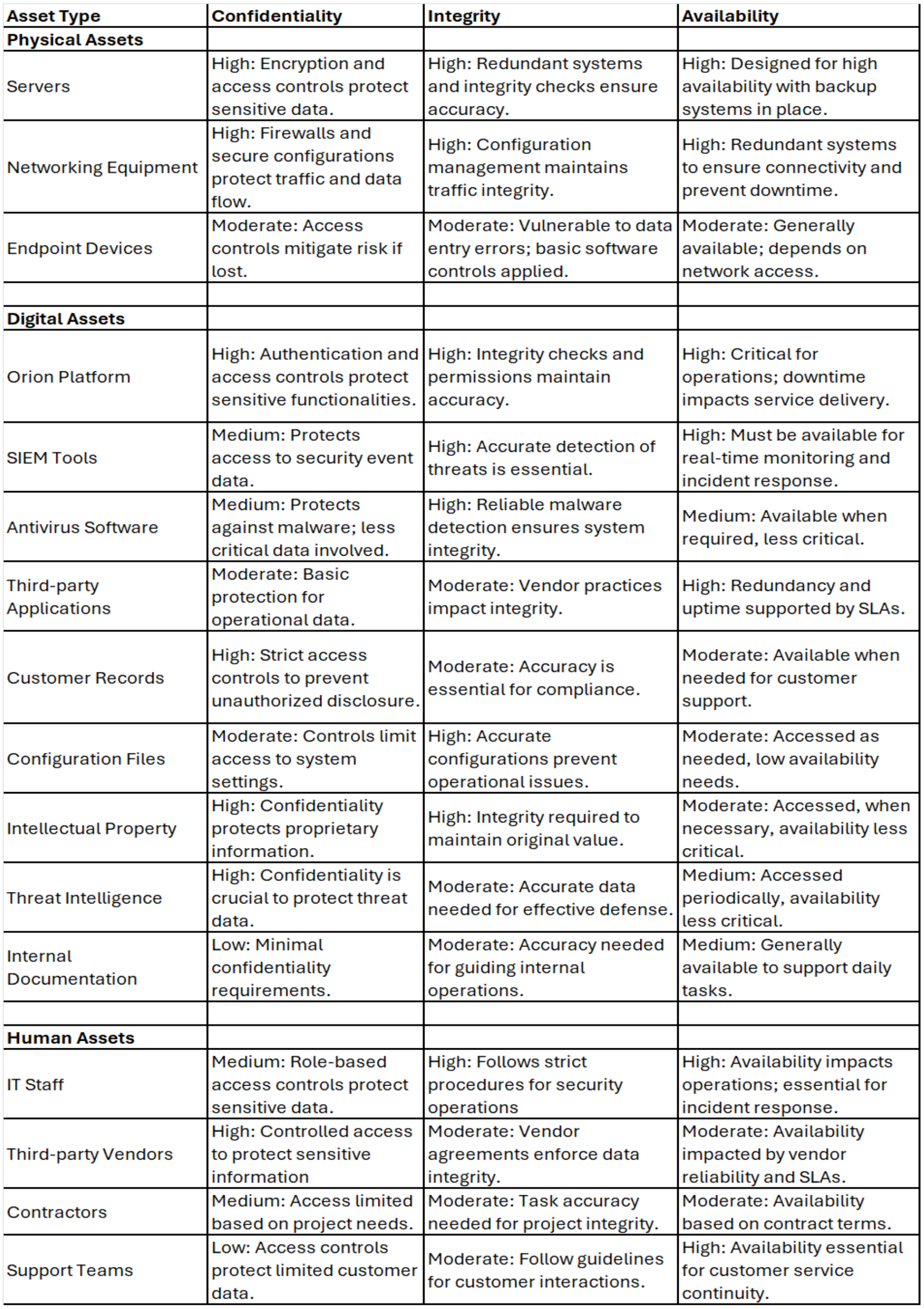
1.2 Asset Categorization:



Asset Type	Description	Category
Physical Assets		
Servers	Hosts applications and data	Critical Infrastructure
Networking Equipment	Enables secure connectivity.	Critical Infrastructure
Endpoint Devices	Workstations and mobile devices.	Moderate Value
Digital Assets		
Orion Platform	Core network monitoring software.	High Value
SIEM Tools	Real-time threat detection and analysis.	High Value
Antivirus Software	Protects against malware and viruses.	High Value
Third-party Applications	Supports monitoring and backups.	Moderate Value
Customer Records	Sensitive customer data.	High Value
Configuration Files	System and software settings.	High Value
Intellectual Property	Proprietary information and code.	High Value
Threat Intelligence	Data on threats and vulnerabilities.	High Value
Internal Documentation	Operational guidelines.	Moderate Value
Human Assets		
IT Staff	Core personnel for maintenance and security.	Critical Resource
Third-party Vendors	Specialized external partners.	Variable Value
Contractors	Temporary personnel for specific tasks.	Moderate Value
Support Teams	Customer-facing personnel.	Moderate Value

The Asset Categorization table organizes SolarWinds' assets by importance, ensuring effective security prioritization. Critical Infrastructure and High Value assets, such as servers, the Orion platform, and customer data, receive the highest protection. Moderate and Variable Value assets support operations but have lower impact on continuity (United States Government Accountability Office, 2021).

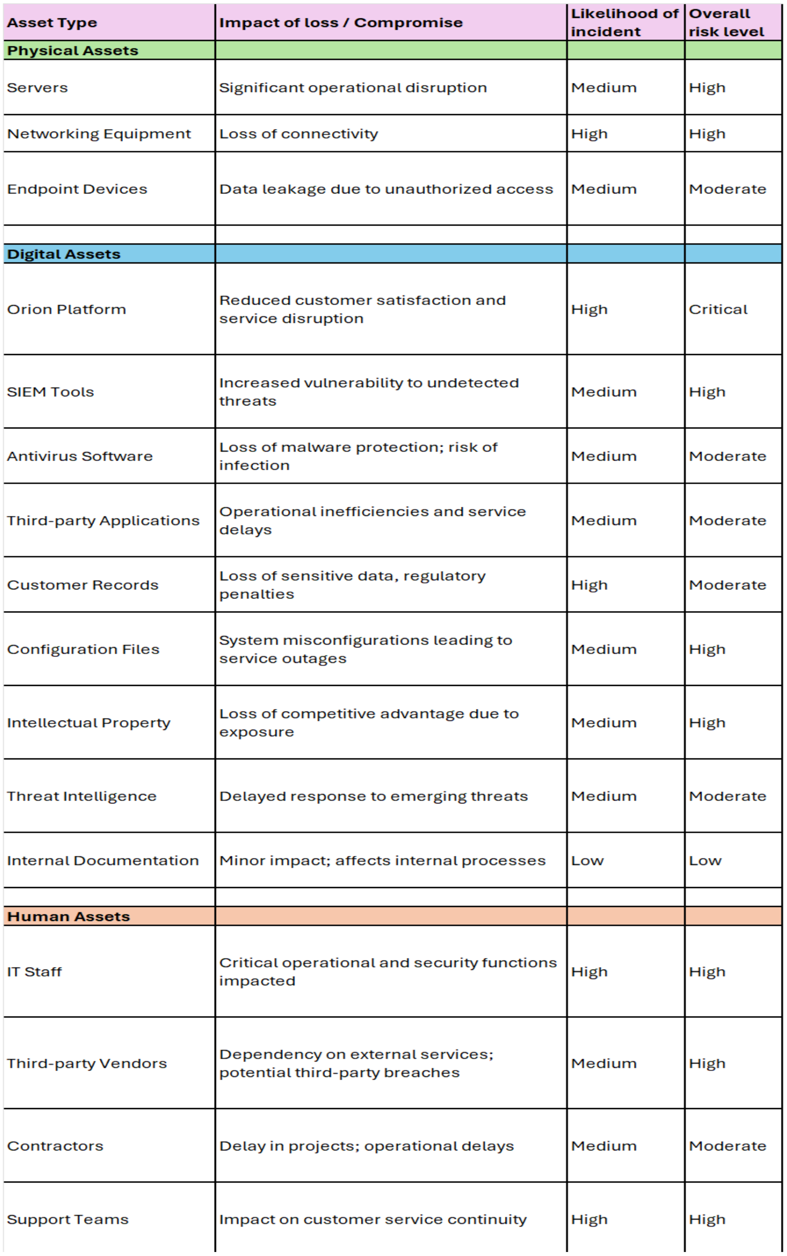
1.3 CIA Triad Evaluation:



Asset Type	Confidentiality	Integrity	Availability
Physical Assets			
Servers	High: Encryption and access controls protect sensitive data.	High: Redundant systems and integrity checks ensure accuracy.	High: Designed for high availability with backup systems in place.
Networking Equipment	High: Firewalls and secure configurations protect traffic and data flow.	High: Configuration management maintains traffic integrity.	High: Redundant systems to ensure connectivity and prevent downtime.
Endpoint Devices	Moderate: Access controls mitigate risk if lost.	Moderate: Vulnerable to data entry errors; basic software controls applied.	Moderate: Generally available; depends on network access.
Digital Assets			
Orion Platform	High: Authentication and access controls protect sensitive functionalities.	High: Integrity checks and permissions maintain accuracy.	High: Critical for operations; downtime impacts service delivery.
SIEM Tools	Medium: Protects access to security event data.	High: Accurate detection of threats is essential.	High: Must be available for real-time monitoring and incident response.
Antivirus Software	Medium: Protects against malware; less critical data involved.	High: Reliable malware detection ensures system integrity.	Medium: Available when required, less critical.
Third-party Applications	Moderate: Basic protection for operational data.	Moderate: Vendor practices impact integrity.	High: Redundancy and uptime supported by SLAs.
Customer Records	High: Strict access controls to prevent unauthorized disclosure.	Moderate: Accuracy is essential for compliance.	Moderate: Available when needed for customer support.
Configuration Files	Moderate: Controls limit access to system settings.	High: Accurate configurations prevent operational issues.	Moderate: Accessed as needed, low availability needs.
Intellectual Property	High: Confidentiality protects proprietary information.	High: Integrity required to maintain original value.	Moderate: Accessed, when necessary, availability less critical.
Threat Intelligence	High: Confidentiality is crucial to protect threat data.	Moderate: Accurate data needed for effective defense.	Medium: Accessed periodically, availability less critical.
Internal Documentation	Low: Minimal confidentiality requirements.	Moderate: Accuracy needed for guiding internal operations.	Medium: Generally available to support daily tasks.
Human Assets			
IT Staff	Medium: Role-based access controls protect sensitive data.	High: Follows strict procedures for security operations	High: Availability impacts operations; essential for incident response.
Third-party Vendors	High: Controlled access to protect sensitive information	Moderate: Vendor agreements enforce data integrity.	Moderate: Availability impacted by vendor reliability and SLAs.
Contractors	Medium: Access limited based on project needs.	Moderate: Task accuracy needed for project integrity.	Moderate: Availability based on contract terms.
Support Teams	Low: Access controls protect limited customer data.	Moderate: Follow guidelines for customer interactions.	High: Availability essential for customer service continuity.

Classification levels (e.g., high, medium, low) are assigned for each asset based on CIA requirements. For instance, the Orion platform would have high confidentiality, integrity, and availability classifications, highlighting its criticality across the triad (Shackleford, 2019).

1.4 Business Impact Analysis:



Asset Type	Impact of loss / Compromise	Likelihood of incident	Overall risk level
Physical Assets			
Servers	Significant operational disruption	Medium	High
Networking Equipment	Loss of connectivity	High	High
Endpoint Devices	Data leakage due to unauthorized access	Medium	Moderate
Digital Assets			
Orion Platform	Reduced customer satisfaction and service disruption	High	Critical
SIEM Tools	Increased vulnerability to undetected threats	Medium	High
Antivirus Software	Loss of malware protection; risk of infection	Medium	Moderate
Third-party Applications	Operational inefficiencies and service delays	Medium	Moderate
Customer Records	Loss of sensitive data, regulatory penalties	High	Moderate
Configuration Files	System misconfigurations leading to service outages	Medium	High
Intellectual Property	Loss of competitive advantage due to exposure	Medium	High
Threat Intelligence	Delayed response to emerging threats	Medium	Moderate
Internal Documentation	Minor impact; affects internal processes	Low	Low
Human Assets			
IT Staff	Critical operational and security functions impacted	High	High
Third-party Vendors	Dependency on external services; potential third-party breaches	Medium	High
Contractors	Delay in projects; operational delays	Medium	Moderate
Support Teams	Impact on customer service continuity	High	High

Business Impact Analysis – Physical Assets (1 example)

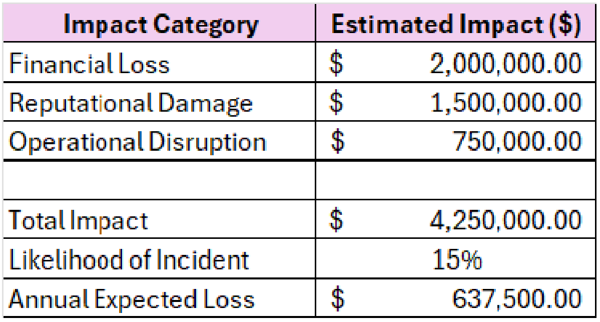
1. *Servers*

Assumptions: Servers are critical for operational continuity, data storage, and core application hosting.

Impact Categories: Financial Loss, Reputational Damage, Operational Disruption.

Estimated Impact Values:

- Financial Loss: $2,000,000 (including potential fines, costs of forensic investigation, and data recovery)
- Reputational Damage: $1,500,000 (impact on customer retention and loss of future revenue)
- Operational Disruption: $750,000 (costs of downtime, backup systems, and IT labor)



Impact Category	Estimated Impact ($)
Financial Loss	$ 2,000,000.00
Reputational Damage	$ 1,500,000.00
Operational Disruption	$ 750,000.00
Total Impact	$ 4,250,000.00
Likelihood of Incident	15%
Annual Expected Loss	$ 637,500.00

Likelihood of Incident: 15% (1 in 6.7 chance of a significant server failure or breach in a year)

Impact Calculation:

- **Total Impact** = Financial Loss + Reputational Damage + Operational Disruption
- **Total Impact** = $2,000,000 + $1,500,000 + $750,000 = $4,250,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident
- **Annual Expected Loss** = $4,250,000 × 0.15 = $637,500

Business Impact Analysis – Digital Assets (1 example)

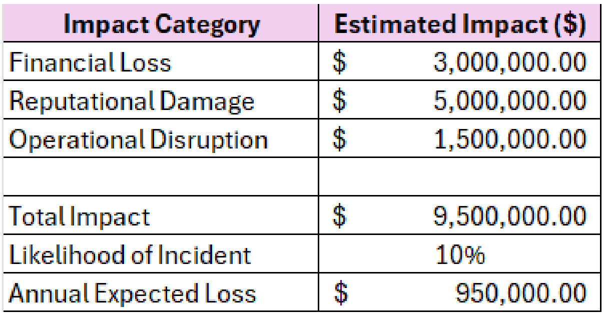
1.Orion Platform

Assumptions: Core product; a critical platform for network monitoring and IT management used by multiple clients.

Impact Categories: Financial Loss, Reputational Damage, Operational Disruption.

Estimated Impact Values:

- Financial Loss: $3,000,000 (includes potential compensation to clients and legal expenses)
- Reputational Damage: $5,000,000 (substantial impact on customer trust and potential loss of future clients)
- Operational Disruption: $1,500,000 (costs related to downtime and recovery efforts)



Impact Category	Estimated Impact ($)
Financial Loss	$ 3,000,000.00
Reputational Damage	$ 5,000,000.00
Operational Disruption	$ 1,500,000.00
Total Impact	$ 9,500,000.00
Likelihood of Incident	10%
Annual Expected Loss	$ 950,000.00

Likelihood of Incident: 10% (1 in 10 chances of a significant disruption or breach annually)

Impact Calculation:

- **Total Impact** = Financial Loss + Reputational Damage + Operational Disruption
- **Total Impact** = $3,000,000 + $5,000,000 + $1,500,000 = $9,500,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident
- **Annual Expected Loss** = $9,500,000 × 0.10 = $950,000

Business Impact Analysis – Human Assets (1 example)

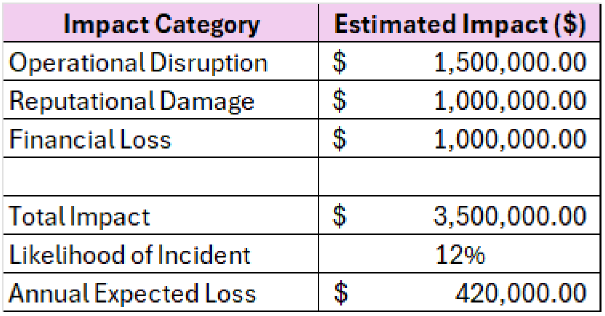
1. IT staff

Assumptions: IT staff are critical for system maintenance, incident response, and cybersecurity management.

Impact Categories: Financial Loss, Reputational Damage, Operational Disruption.

Estimated Impact Values:

- Financial Loss: $1,000,000 (increased costs to hire and train new personnel, overtime pay, and outsourcing expenses)
- Reputational Damage: $1,000,000 (client trust compromised if security is not effectively managed)
- Operational Disruption: $1,500,000 (loss of IT staff affects system availability, maintenance, and security incident response)



Impact Category	Estimated Impact ($)
Operational Disruption	$ 1,500,000.00
Reputational Damage	$ 1,000,000.00
Financial Loss	$ 1,000,000.00
Total Impact	$ 3,500,000.00
Likelihood of Incident	12%
Annual Expected Loss	$ 420,000.00

Likelihood of Incident: 12% (1 in 8.3 chance of key IT staff loss or unavailability in a year)

Impact Calculation:

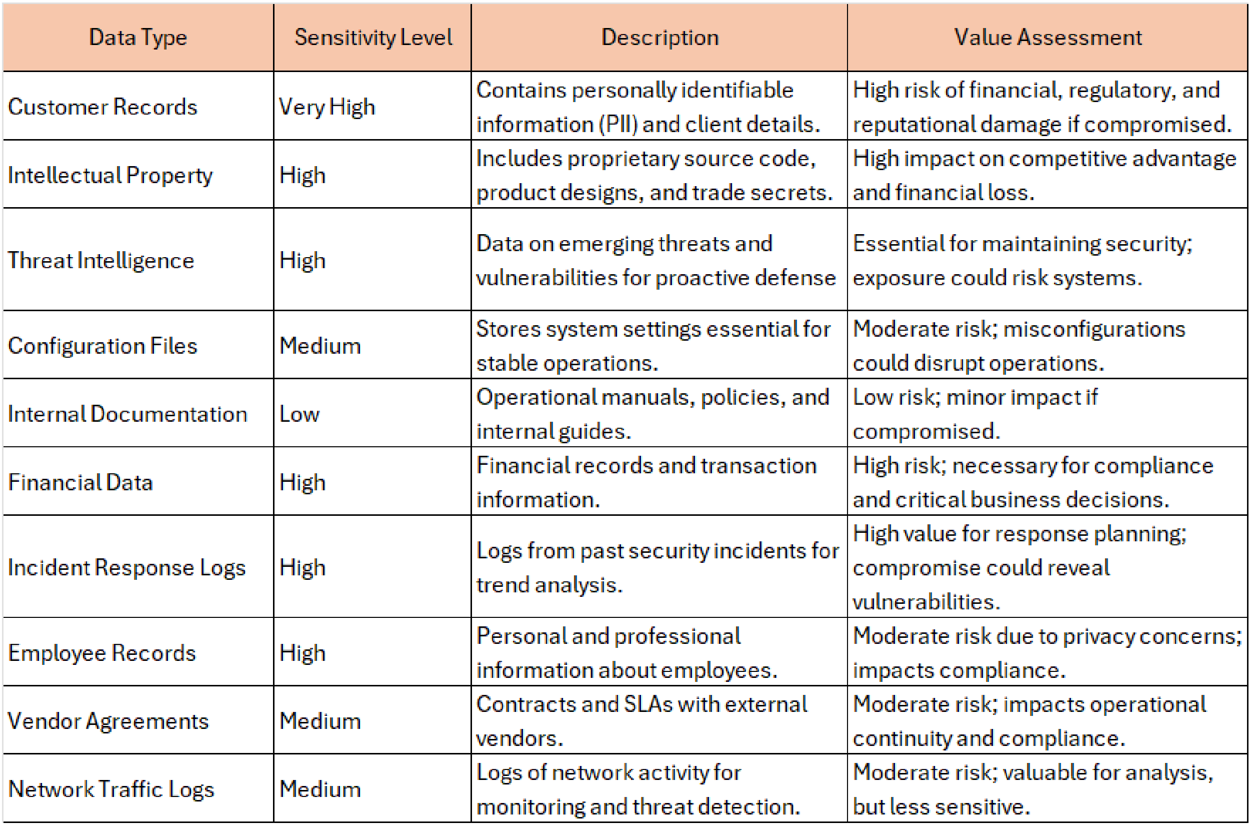
- **Total Impact** = Financial Loss + Reputational Damage + Operational Disruption
- **Total Impact** = $1,000,000 + $1,000,000 + $1,500,000 = $3,500,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident
- **Annual Expected Loss** = $3,500,000 × 0.12 = $420,000

***** Please see Appendix A for detail analysis for all assets*****

1.5 Data Sensitivity and Value Assessment:



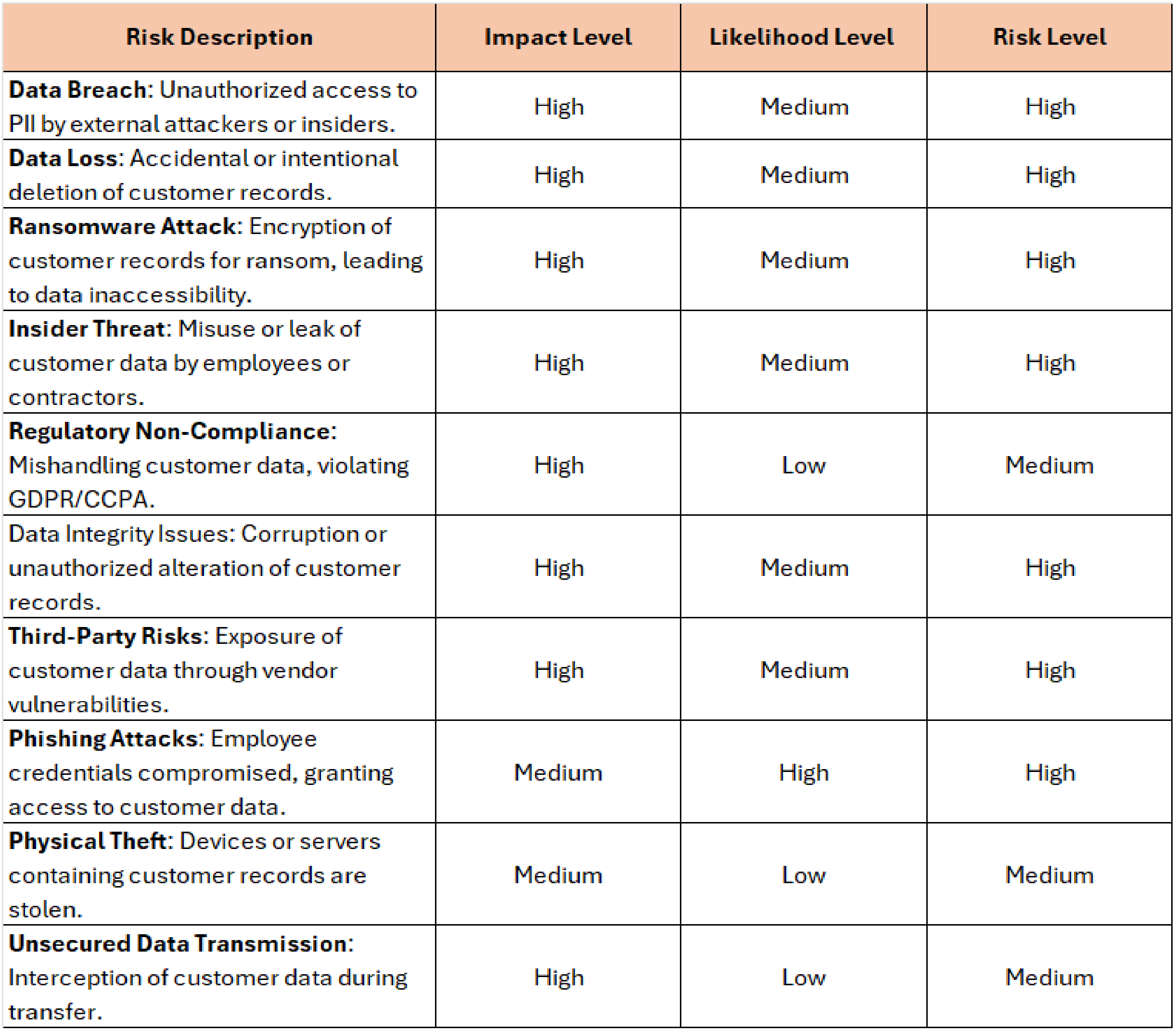
Data Type	Sensitivity Level	Description	Value Assessment
Customer Records	Very High	Contains personally identifiable information (PII) and client details.	High risk of financial, regulatory, and reputational damage if compromised.
Intellectual Property	High	Includes proprietary source code, product designs, and trade secrets.	High impact on competitive advantage and financial loss.
Threat Intelligence	High	Data on emerging threats and vulnerabilities for proactive defense	Essential for maintaining security; exposure could risk systems.
Configuration Files	Medium	Stores system settings essential for stable operations.	Moderate risk; misconfigurations could disrupt operations.
Internal Documentation	Low	Operational manuals, policies, and internal guides.	Low risk; minor impact if compromised.
Financial Data	High	Financial records and transaction information.	High risk; necessary for compliance and critical business decisions.
Incident Response Logs	High	Logs from past security incidents for trend analysis.	High value for response planning; compromise could reveal vulnerabilities.
Employee Records	High	Personal and professional information about employees.	Moderate risk due to privacy concerns; impacts compliance.
Vendor Agreements	Medium	Contracts and SLAs with external vendors.	Moderate risk; impacts operational continuity and compliance.
Network Traffic Logs	Medium	Logs of network activity for monitoring and threat detection.	Moderate risk; valuable for analysis, but less sensitive.

Assets are classified based on the data they handle and the potential impact of data breaches. For example, data related to customer records is highly sensitive, warranting the highest level of security. This table can help to guide security resource allocation, ensuring that the most critical data receives robust protection (National Institute of Standards and Technology [NIST], 2018).

Component 2: Developing Methods for evaluating and monitoring Cyber Risk Management

we will use customer record as example in component 2 since customer records are classified as very high sensitivity in term of both financial impact and regulatory implications. This data contains Personally Identifiable Information (PII) and is subject to stringent regulatory requirements which make it a high-priority asset in any risk management program (The SANS Institute, 2021).

2.1 Qualitative Risk Assessment:



Risk Description	Impact Level	Likelihood Level	Risk Level
Data Breach: Unauthorized access to PII by external attackers or insiders.	High	Medium	High
Data Loss: Accidental or intentional deletion of customer records.	High	Medium	High
Ransomware Attack: Encryption of customer records for ransom, leading to data inaccessibility.	High	Medium	High
Insider Threat: Misuse or leak of customer data by employees or contractors.	High	Medium	High
Regulatory Non-Compliance: Mishandling customer data, violating GDPR/CCPA.	High	Low	Medium
Data Integrity Issues: Corruption or unauthorized alteration of customer records.	High	Medium	High
Third-Party Risks: Exposure of customer data through vendor vulnerabilities.	High	Medium	High
Phishing Attacks: Employee credentials compromised, granting access to customer data.	Medium	High	High
Physical Theft: Devices or servers containing customer records are stolen.	Medium	Low	Medium
Unsecured Data Transmission: Interception of customer data during transfer.	High	Low	Medium

The goal of qualitative risk assessment for customer records is to identify and prioritize risk through expert judgment and utilizing risk matrix. Working with cybersecurity experts helps identify potential threats (i.e. data breaches, ransomware, and insider threats) to customer records. Each risk is evaluated using a risk matrix based on impact and likelihood, with high-priority risks (e.g., unauthorized access, data loss) assigned an overall risk level (e.g., high or medium). This process provides a clear understanding of critical risks, enabling SolarWinds to implement targeted security measures to safeguard customer records effectively (National Institute of Standards and Technology [NIST], 2018).

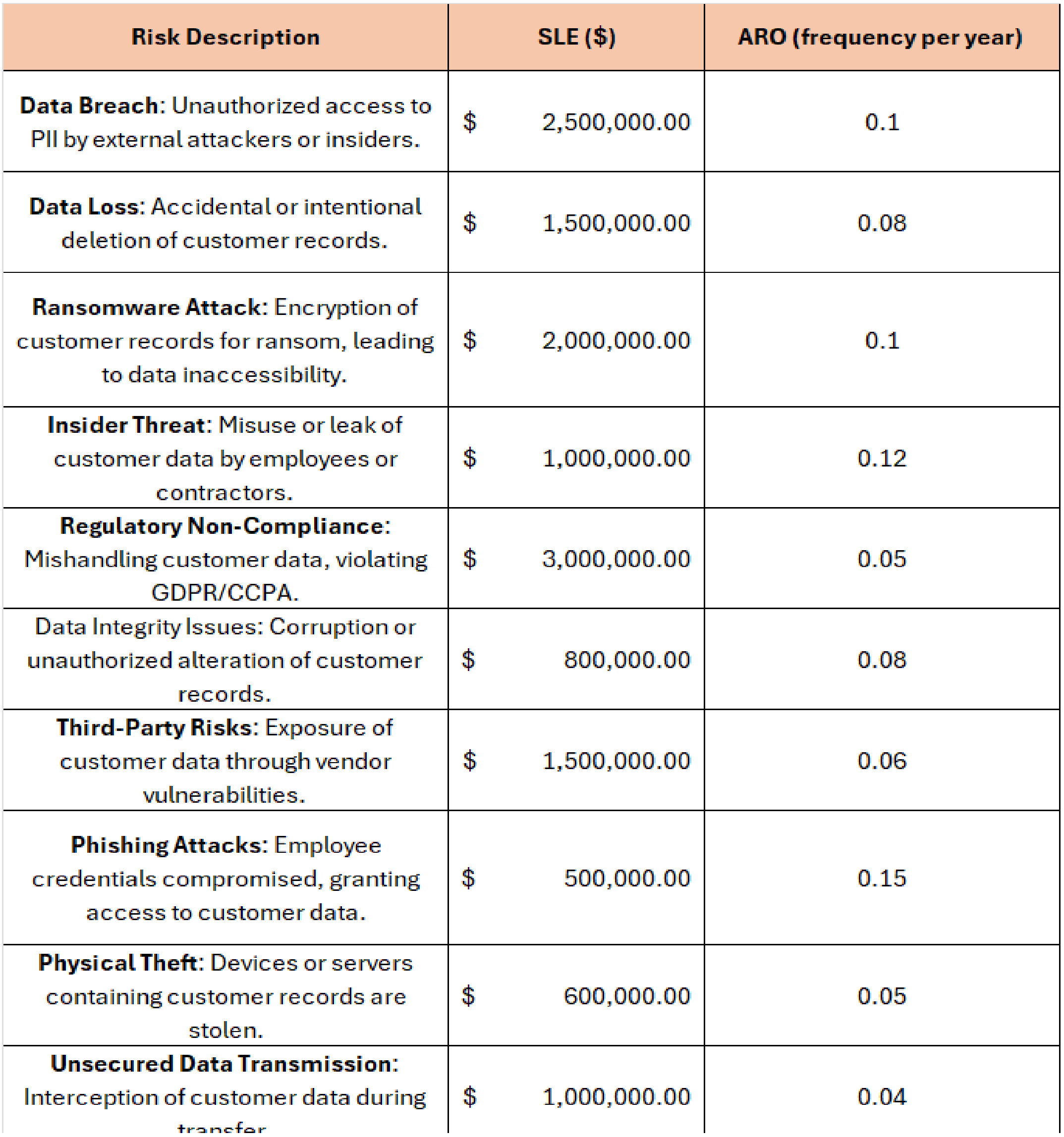
2.2 Quantitative Risk Assessment:

Identify Risks and Determine Potential Impact

Using risk descriptions from qualitative risk assessment, we can consider the following risks to customer records:

- Data Breach
- Data Loss
- Ransomware Attack
- Insider Threat
- Regulatory Non-Compliance
- Data Integrity Issues
- Third-Party Risks
- Phishing Attacks
- Physical Theft
- Unsecured Data Transmission

Assign Values (Using Single Loss Expectancy (SLE) and Annual Rate of Occurrence (ARO))



Risk Description	SLE ($)	ARO (frequency per year)
Data Breach: Unauthorized access to PII by external attackers or insiders.	$ 2,500,000.00	0.1
Data Loss: Accidental or intentional deletion of customer records.	$ 1,500,000.00	0.08
Ransomware Attack: Encryption of customer records for ransom, leading to data inaccessibility.	$ 2,000,000.00	0.1
Insider Threat: Misuse or leak of customer data by employees or contractors.	$ 1,000,000.00	0.12
Regulatory Non-Compliance: Mishandling customer data, violating GDPR/CCPA.	$ 3,000,000.00	0.05
Data Integrity Issues: Corruption or unauthorized alteration of customer records.	$ 800,000.00	0.08
Third-Party Risks: Exposure of customer data through vendor vulnerabilities.	$ 1,500,000.00	0.06
Phishing Attacks: Employee credentials compromised, granting access to customer data.	$ 500,000.00	0.15
Physical Theft: Devices or servers containing customer records are stolen.	$ 600,000.00	0.05
Unsecured Data Transmission: Interception of customer data during transfer	$ 1,000,000.00	0.04

Calculate Annual Loss Expectancy (ALE)

The formula for calculating ALE is **ALE = SLE × ARO**

Data Breach: $\$ 2{,}500{,}000 \times 0.10 = \$ 250{,}000$

Data Loss: $\$ 1{,}500{,}000 \times 0.08 = \$ 120{,}000$

Ransomware Attack: $\$ 2{,}000{,}000 \times 0.10 = \$ 200{,}000$

Insider Threat: $\$ 1{,}000{,}000 \times 0.12 = \$ 120{,}000$

Regulatory Non-Compliance: $\$ 3{,}000{,}000 \times 0.05 = \$ 150{,}000$

Data Integrity Issues: $\$ 800{,}000 \times 0.08 = \$ 64{,}000$

Third-Party Risks: $\$ 1{,}500{,}000 \times 0.06 = \$ 90{,}000$

Phishing Attacks: $\$ 500{,}000 \times 0.15 = \$ 75{,}000$

Physical Theft: $\$ 600{,}000 \times 0.05 = \$ 30{,}000$

Unsecured Data Transmission: $\$ 1{,}000{,}000 \times 0.04 = \$ 40{,}000$

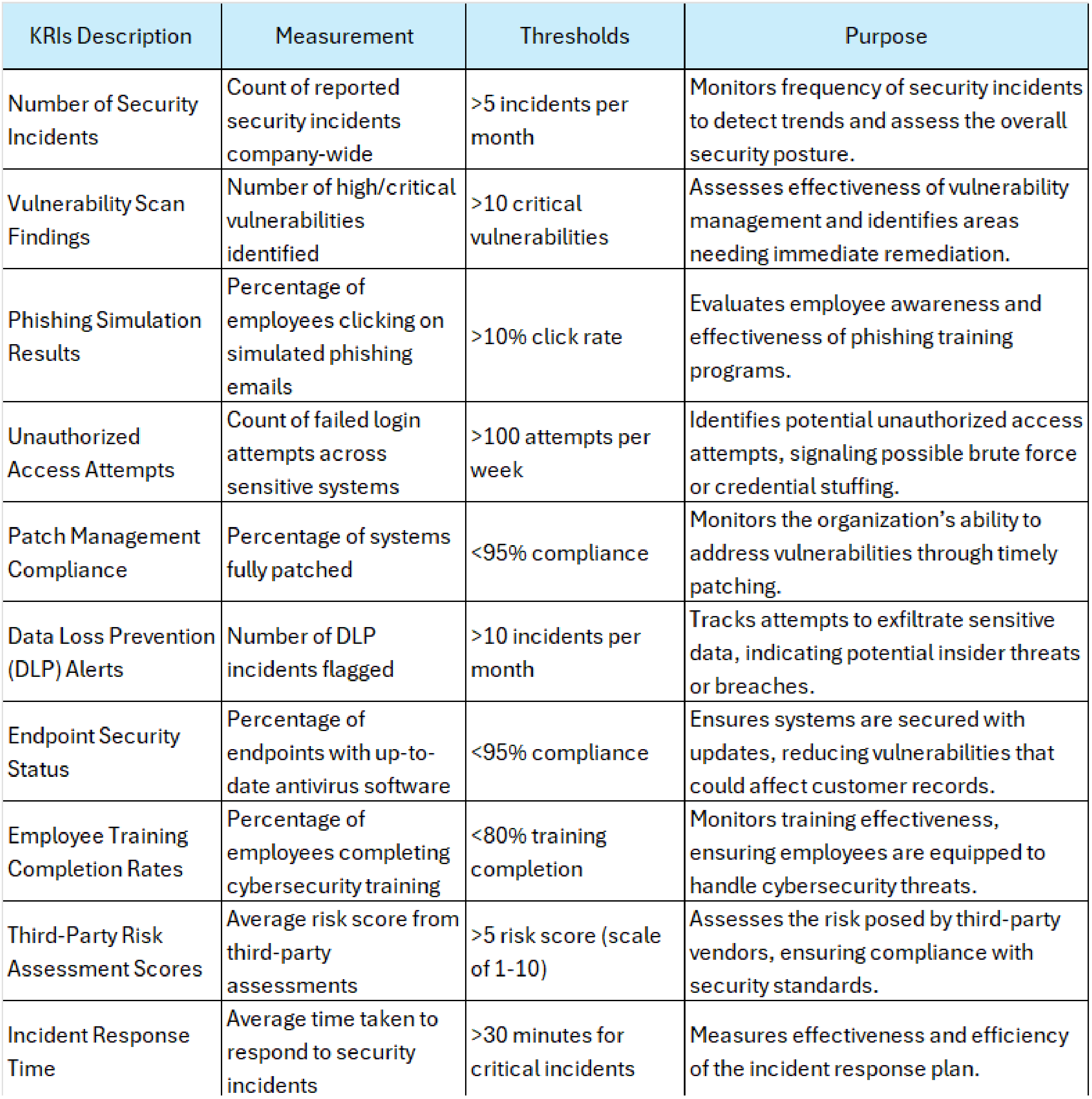
Total Annual Loss Expectancy (ALE)

Total ALE = Sum of all individual ALEs (Gordon, Loeb, & Zhou, 2011)

$$Total\ ALE = \$ 250{,}000 + \$ 120{,}000 + \$ 200{,}000 + \$ 120{,}000 + \$ 150{,}000 + \$ 64{,}000 + \$ 90{,}000 + \$ 75{,}000 + \$ 30{,}000 + \$ 40{,}000$$

$$Total\ ALE = \$ 1{,}139{,}000$$

2.3 Key Risk Indicators (KRIs) for SolarWinds Corporation:



KRIs Description	Measurement	Thresholds	Purpose
Number of Security Incidents	Count of reported security incidents company-wide	>5 incidents per month	Monitors frequency of security incidents to detect trends and assess the overall security posture.
Vulnerability Scan Findings	Number of high/critical vulnerabilities identified	>10 critical vulnerabilities	Assesses effectiveness of vulnerability management and identifies areas needing immediate remediation.
Phishing Simulation Results	Percentage of employees clicking on simulated phishing emails	>10% click rate	Evaluates employee awareness and effectiveness of phishing training programs.
Unauthorized Access Attempts	Count of failed login attempts across sensitive systems	>100 attempts per week	Identifies potential unauthorized access attempts, signaling possible brute force or credential stuffing.
Patch Management Compliance	Percentage of systems fully patched	<95% compliance	Monitors the organization's ability to address vulnerabilities through timely patching.
Data Loss Prevention (DLP) Alerts	Number of DLP incidents flagged	>10 incidents per month	Tracks attempts to exfiltrate sensitive data, indicating potential insider threats or breaches.
Endpoint Security Status	Percentage of endpoints with up-to-date antivirus software	<95% compliance	Ensures systems are secured with updates, reducing vulnerabilities that could affect customer records.
Employee Training Completion Rates	Percentage of employees completing cybersecurity training	<80% training completion	Monitors training effectiveness, ensuring employees are equipped to handle cybersecurity threats.
Third-Party Risk Assessment Scores	Average risk score from third-party assessments	>5 risk score (scale of 1-10)	Assesses the risk posed by third-party vendors, ensuring compliance with security standards.
Incident Response Time	Average time taken to respond to security incidents	>30 minutes for critical incidents	Measures effectiveness and efficiency of the incident response plan.

These KRIs will provide SolarWinds with a comprehensive view of organizational risks that helps to detect potential threats early and manage threat effectively. By having clear measurements and thresholds, SolarWinds can identify trends, adjust strategies, and ensure a robust cybersecurity posture across the organization (Center for Internet Security, 2020).

2.4 Continuous Monitoring Plan:

Purpose

To proactively monitor and protect SolarWinds' assets by identifying and addressing cybersecurity threats in real-time. This plan aims to minimize risks related to unauthorized access, data breaches, and malware by implementing an integrated monitoring strategy across the organization (Shackleford, 2019).

Objective

To establish a robust continuous monitoring framework that provides real-time visibility into potential cyber threats that allow SolarWinds to detect, analyze, and respond swiftly to security incidents which ensure the safety and integrity of critical assets.

Scope

This monitoring plan covers all critical assets, including customer records, infrastructure, network traffic, and endpoint devices. It applies to on-premises, cloud, and third-party environments, encompassing SolarWinds' internal IT systems, third-party integrations, and data storage solutions. The plan involves the deployment and maintenance of tools such as SIEM, EDR, Network Traffic Analysis, reviewing and vulnerability scanners (Heiser & Nicolett, 2020) (SolarWinds Corporation, 2021).

Key Components of the Continuous Monitoring Plan

Security Information and Event Management (SIEM)

Implement a SIEM solution to aggregate logs from multiple sources (e.g., firewalls, servers, applications), enabling real-time monitoring and analysis of security events (SolarWinds Corporation, 2021).

- **Frequency**: Continuous monitoring, with weekly reviews of logs and alerts.
- **Responsibility**: SOC Team.

Endpoint Detection and Response (EDR)

Deploy EDR solutions to monitor and protect endpoint devices (e.g., laptops, desktops, servers) from malware and suspicious activities.

- **Frequency**: Continuous monitoring of endpoints, with daily checks for alerts.
- **Responsibility**: SOC and IT Security Teams.

Network Traffic Analysis (NTA)

Continuously monitor network traffic patterns to detect anomalies, such as unexpected data flows or unusual access to critical servers.

- **Frequency**: Real-time monitoring with quarterly reviews of traffic baselines.
- **Responsibility**: Network Security Team.

Threat Intelligence Feeds

Subscribe to threat intelligence feeds and services to gather insights on emerging threats, vulnerabilities, and attack vectors relevant to SolarWinds' industry.

- **Frequency**: Daily monitoring and analysis of threat intelligence.
- **Responsibility**: Security Operations Center (SOC) team.

Vulnerability Scanning and Patch Management

Conduct regular vulnerability scans across systems and applications to identify and address security weaknesses.

- **Frequency**: Monthly scans, with additional ad-hoc scans after significant system changes or incidents.
- **Responsibility**: IT Security Team.

Reporting and Metrics

- Develop regular reports summarizing the findings from continuous monitoring activities, including incidents, vulnerabilities, and compliance status.
- Monthly security reports, with additional executive briefings quarterly.

Review and Improvement

- Conduct an annual review of the Continuous Monitoring Plan to ensure its effectiveness and relevance to evolving threats.
- Providing a feedback mechanism to incorporate lessons learned from incidents.

Implementation of the Monitoring Plan

1. *Initial Setup and Configuration*

- Deploying and configuring each monitoring tool based on SolarWinds' specific infrastructure and assets.
- Defining baseline thresholds and alert levels for each tool that considers the organization's risk tolerance.
- Training cybersecurity staff on the use of monitoring tools and response protocols.

2. *Integration and Centralized Management*

- Integrating SIEM as the central console, pulling data from IDS/IPS, EDR, NTA, and threat intelligence feeds.
- Establishing centralized dashboards and automated reporting for quick visibility into potential threats across all systems.
- Configuring escalation paths for alerts to ensure swift response to high-priority incidents.

3. *Incident Response*

- Defining alert thresholds for critical incidents, which enable priority alerts to incident response teams immediately.
- Developing standard operating procedures (SOPs) for each type of alert, specifying steps for investigation, containment, and remediation.

4. *Staff Training and Awareness*

- Conducting training sessions for cybersecurity and IT teams on responding to alerts and using monitoring tools effectively.
- Ensuring all employees understand basic security hygiene and how their activities contribute to the overall security posture.

5. *Continuous Improvement and Review*

- Performing periodic reviews of all monitoring tools to ensure they remain aligned with evolving threats.
- Conducting quarterly assessments of incident response times and adjusting alert thresholds as needed.

- Solicit feedback from incident response teams to improve alert accuracy and reduce false positives (Heiser & Nicolett, 2020)..

Maintenance of the Monitoring Plan

Regular Updates: Keep all tools up to date with the latest patches, rule sets, and signatures to ensure they address current threats.

Annually Reviews: Reassess monitoring rules, thresholds, and alert configurations based on recent incidents and emerging threat intelligence.

Documentation and Reporting: Document all updates, incident responses, and changes to the monitoring setup. Provide regular reports to stakeholders on monitoring effectiveness and any areas for improvement.

Performance Metrics: Track metrics like incident response time, number of false positives, and average detection time to measure the effectiveness of the monitoring plan (Sonnenreich, Albanese, & Stout, 2006).

2.5 Periodic Risk Assessment Plan:

The purpose is to establish a structured approach to conducting regular risk assessments that identify, evaluate, and mitigate risks to SolarWinds' critical assets and operations.

Frequency of Risk Assessments

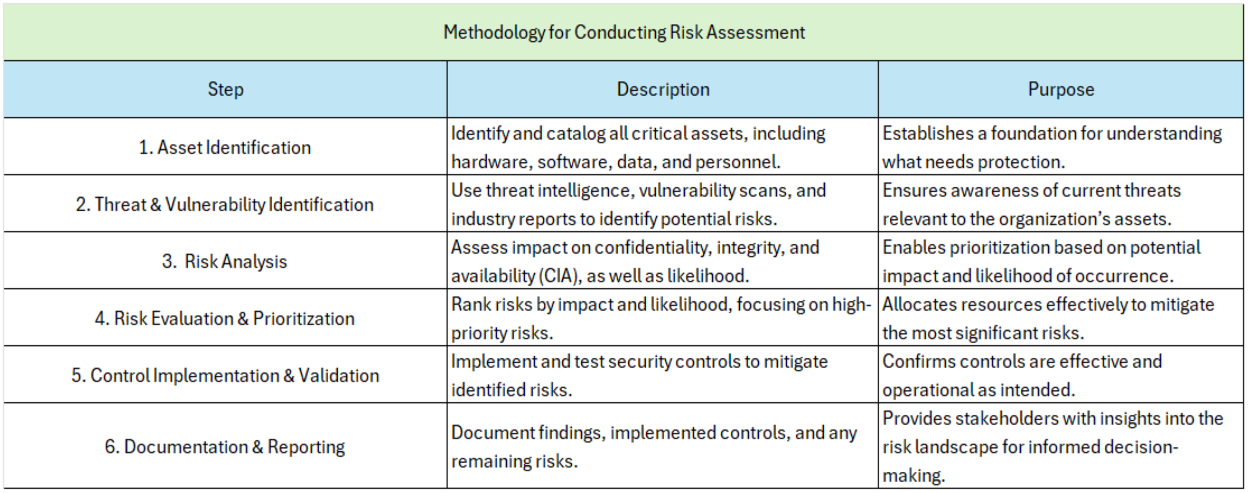
Annual Comprehensive Risk Assessment: Full assessment of all critical assets each year.

Quarterly Risk Reviews: Targeted reviews of high-risk areas and checking for emerging threat every three months.

Ad-hoc Assessments: Additional assessments triggered by major changes in threat landscape, after incidents, major upgrades or regulatory requirements (Radvanovsky & McDougall, 2018).

Activity	Frequency	Responsible party
Annual Comprehensive Risk Assessment	Annually	Risk Management Team
Quarterly Risk Reviews	Quarterly	SOC Team
Ad-hoc Assessments	As required	Relevant Teams
Stakeholder Interviews	Each assessment	Risk Management Team
Management Review & Reporting	After each assessment	Senior Management

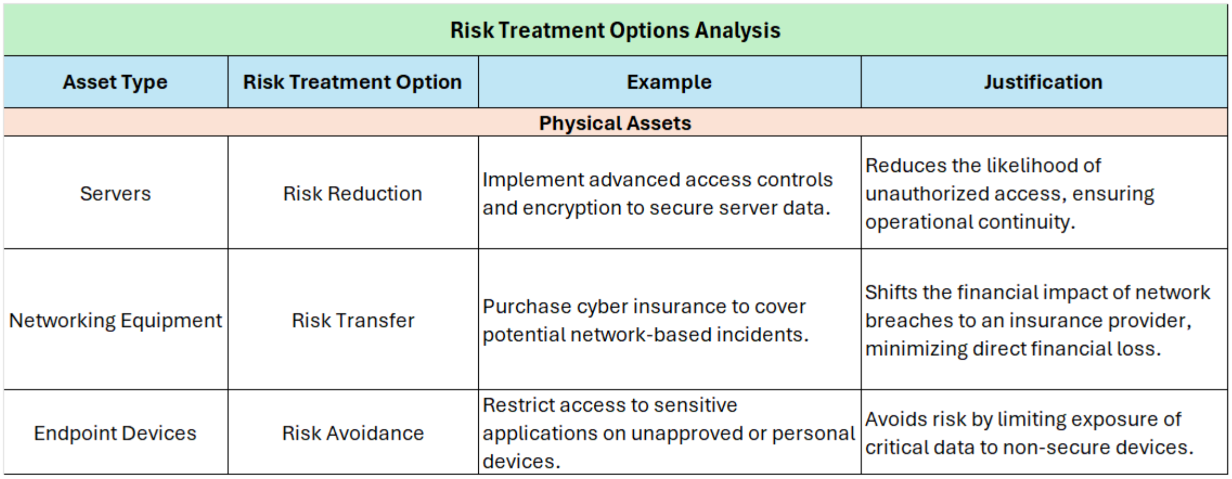
Methodology for Conducting Risk Assessment



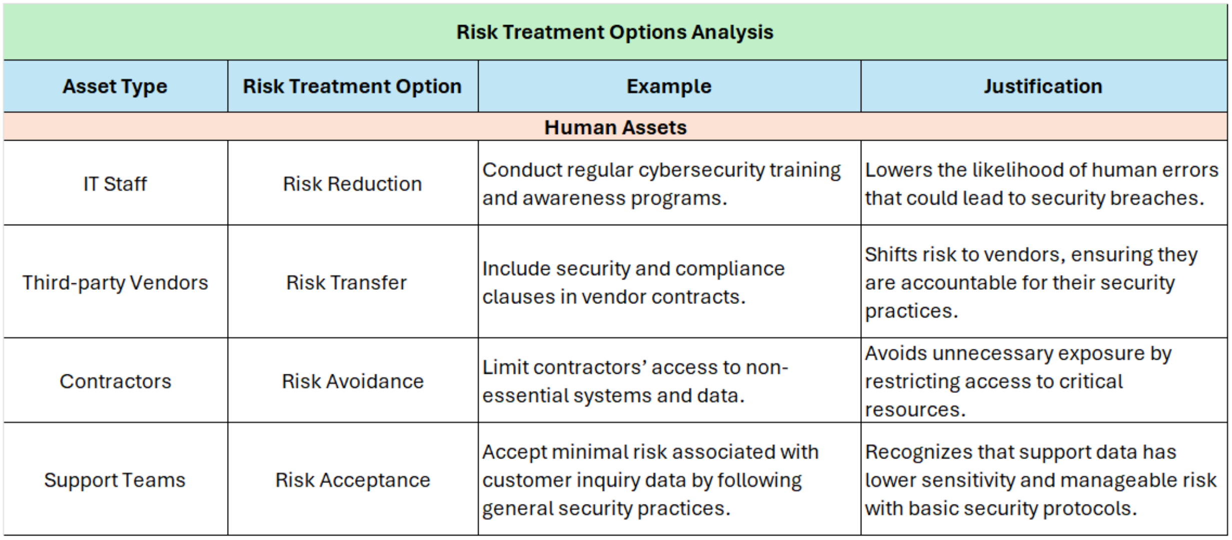
Methodology for Conducting Risk Assessment		
Step	Description	Purpose
1. Asset Identification	Identify and catalog all critical assets, including hardware, software, data, and personnel.	Establishes a foundation for understanding what needs protection.
2. Threat & Vulnerability Identification	Use threat intelligence, vulnerability scans, and industry reports to identify potential risks.	Ensures awareness of current threats relevant to the organization's assets.
3. Risk Analysis	Assess impact on confidentiality, integrity, and availability (CIA), as well as likelihood.	Enables prioritization based on potential impact and likelihood of occurrence.
4. Risk Evaluation & Prioritization	Rank risks by impact and likelihood, focusing on high-priority risks.	Allocates resources effectively to mitigate the most significant risks.
5. Control Implementation & Validation	Implement and test security controls to mitigate identified risks.	Confirms controls are effective and operational as intended.
6. Documentation & Reporting	Document findings, implemented controls, and any remaining risks.	Provides stakeholders with insights into the risk landscape for informed decision-making.

Component 3: Determining Cost Effectiveness Treatments to Manage Cyber Risk

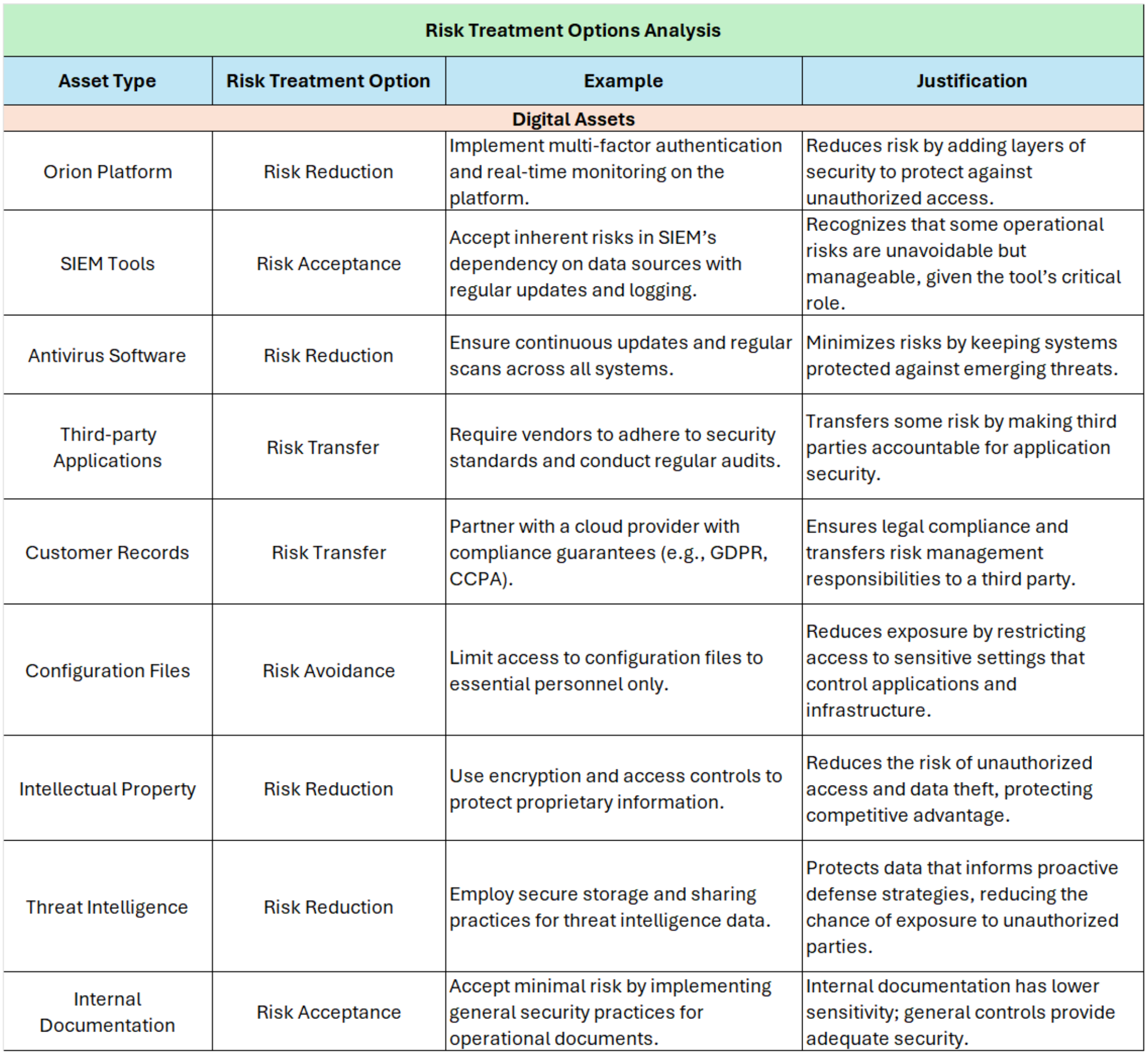
3.1 Risk treatment options Analysis:



Risk Treatment Options Analysis			
Asset Type	**Risk Treatment Option**	**Example**	**Justification**
Physical Assets			
Servers	Risk Reduction	Implement advanced access controls and encryption to secure server data.	Reduces the likelihood of unauthorized access, ensuring operational continuity.
Networking Equipment	Risk Transfer	Purchase cyber insurance to cover potential network-based incidents.	Shifts the financial impact of network breaches to an insurance provider, minimizing direct financial loss.
Endpoint Devices	Risk Avoidance	Restrict access to sensitive applications on unapproved or personal devices.	Avoids risk by limiting exposure of critical data to non-secure devices.



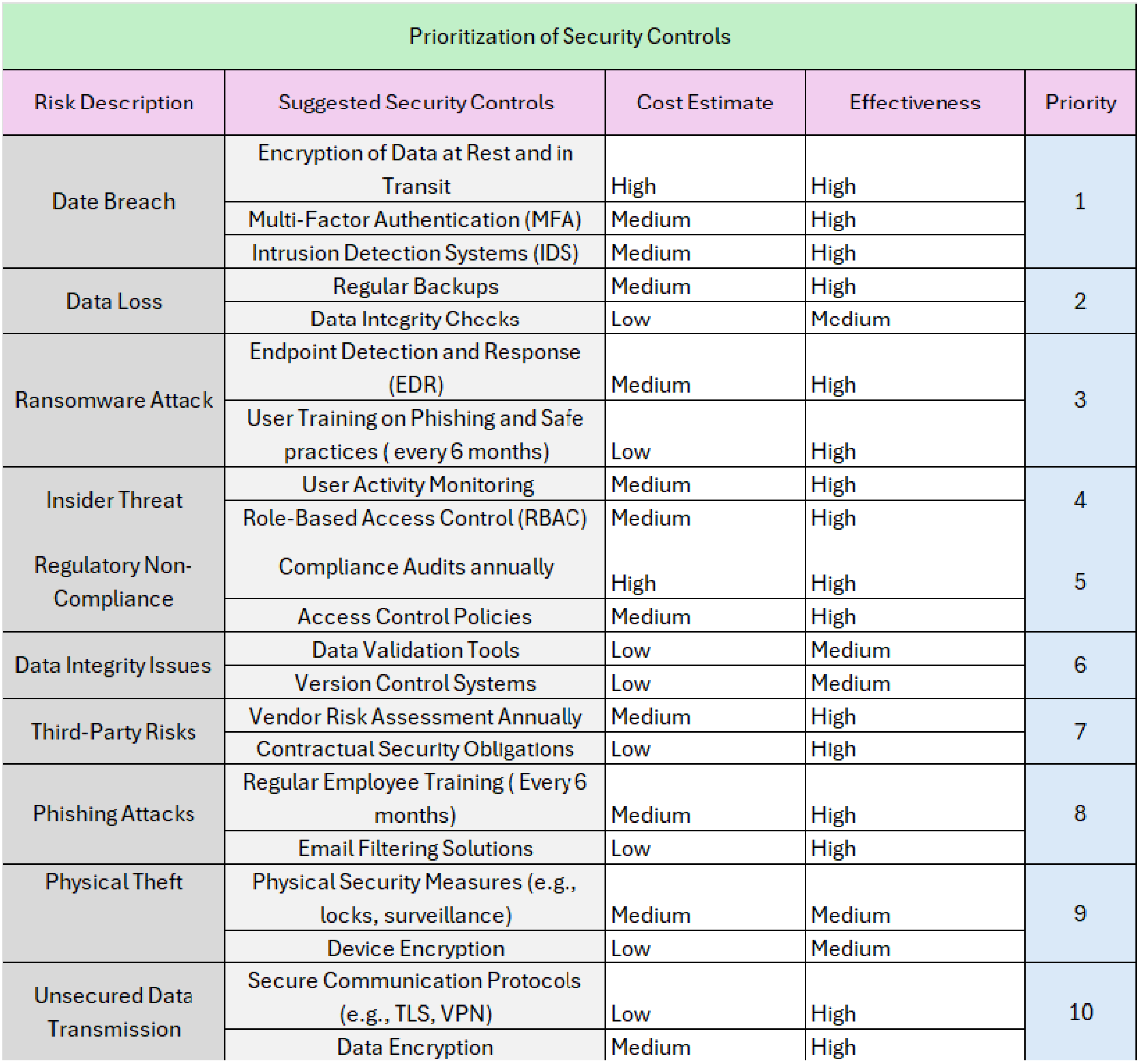
Risk Treatment Options Analysis			
Asset Type	**Risk Treatment Option**	**Example**	**Justification**
Human Assets			
IT Staff	Risk Reduction	Conduct regular cybersecurity training and awareness programs.	Lowers the likelihood of human errors that could lead to security breaches.
Third-party Vendors	Risk Transfer	Include security and compliance clauses in vendor contracts.	Shifts risk to vendors, ensuring they are accountable for their security practices.
Contractors	Risk Avoidance	Limit contractors' access to non-essential systems and data.	Avoids unnecessary exposure by restricting access to critical resources.
Support Teams	Risk Acceptance	Accept minimal risk associated with customer inquiry data by following general security practices.	Recognizes that support data has lower sensitivity and manageable risk with basic security protocols.



Risk Treatment Options Analysis

Asset Type	Risk Treatment Option	Example	Justification
Digital Assets			
Orion Platform	Risk Reduction	Implement multi-factor authentication and real-time monitoring on the platform.	Reduces risk by adding layers of security to protect against unauthorized access.
SIEM Tools	Risk Acceptance	Accept inherent risks in SIEM's dependency on data sources with regular updates and logging.	Recognizes that some operational risks are unavoidable but manageable, given the tool's critical role.
Antivirus Software	Risk Reduction	Ensure continuous updates and regular scans across all systems.	Minimizes risks by keeping systems protected against emerging threats.
Third-party Applications	Risk Transfer	Require vendors to adhere to security standards and conduct regular audits.	Transfers some risk by making third parties accountable for application security.
Customer Records	Risk Transfer	Partner with a cloud provider with compliance guarantees (e.g., GDPR, CCPA).	Ensures legal compliance and transfers risk management responsibilities to a third party.
Configuration Files	Risk Avoidance	Limit access to configuration files to essential personnel only.	Reduces exposure by restricting access to sensitive settings that control applications and infrastructure.
Intellectual Property	Risk Reduction	Use encryption and access controls to protect proprietary information.	Reduces the risk of unauthorized access and data theft, protecting competitive advantage.
Threat Intelligence	Risk Reduction	Employ secure storage and sharing practices for threat intelligence data.	Protects data that informs proactive defense strategies, reducing the chance of exposure to unauthorized parties.
Internal Documentation	Risk Acceptance	Accept minimal risk by implementing general security practices for operational documents.	Internal documentation has lower sensitivity; general controls provide adequate security.

3.2 Prioritization of Security Controls:



Prioritization of Security Controls				
Risk Description	Suggested Security Controls	Cost Estimate	Effectiveness	Priority
Date Breach	Encryption of Data at Rest and in Transit	High	High	1
	Multi-Factor Authentication (MFA)	Medium	High	
	Intrusion Detection Systems (IDS)	Medium	High	
Data Loss	Regular Backups	Medium	High	2
	Data Intcgrity Chccks	Low	Mcdium	
Ransomware Attack	Endpoint Detection and Response (EDR)	Medium	High	3
	User Training on Phishing and Safe practices (every 6 months)	Low	High	
Insider Threat	User Activity Monitoring	Medium	High	4
	Role-Based Access Control (RBAC)	Medium	High	
Regulatory Non-Compliance	Compliance Audits annually	High	High	5
	Access Control Policies	Medium	High	
Data Integrity Issues	Data Validation Tools	Low	Medium	6
	Version Control Systems	Low	Medium	
Third-Party Risks	Vendor Risk Assessment Annually	Medium	High	7
	Contractual Securlty Obllgatlons	Low	Hlgh	
Phishing Attacks	Regular Employee Training (Every 6 months)	Medium	High	8
	Email Filtering Solutions	Low	High	
Physical Theft	Physical Security Measures (e.g., locks, surveillance)	Medium	Medium	9
	Device Encryption	Low	Medium	
Unsecured Data Transmission	Secure Communication Protocols (e.g., TLS, VPN)	Low	High	10
	Data Encryption	Medium	High	

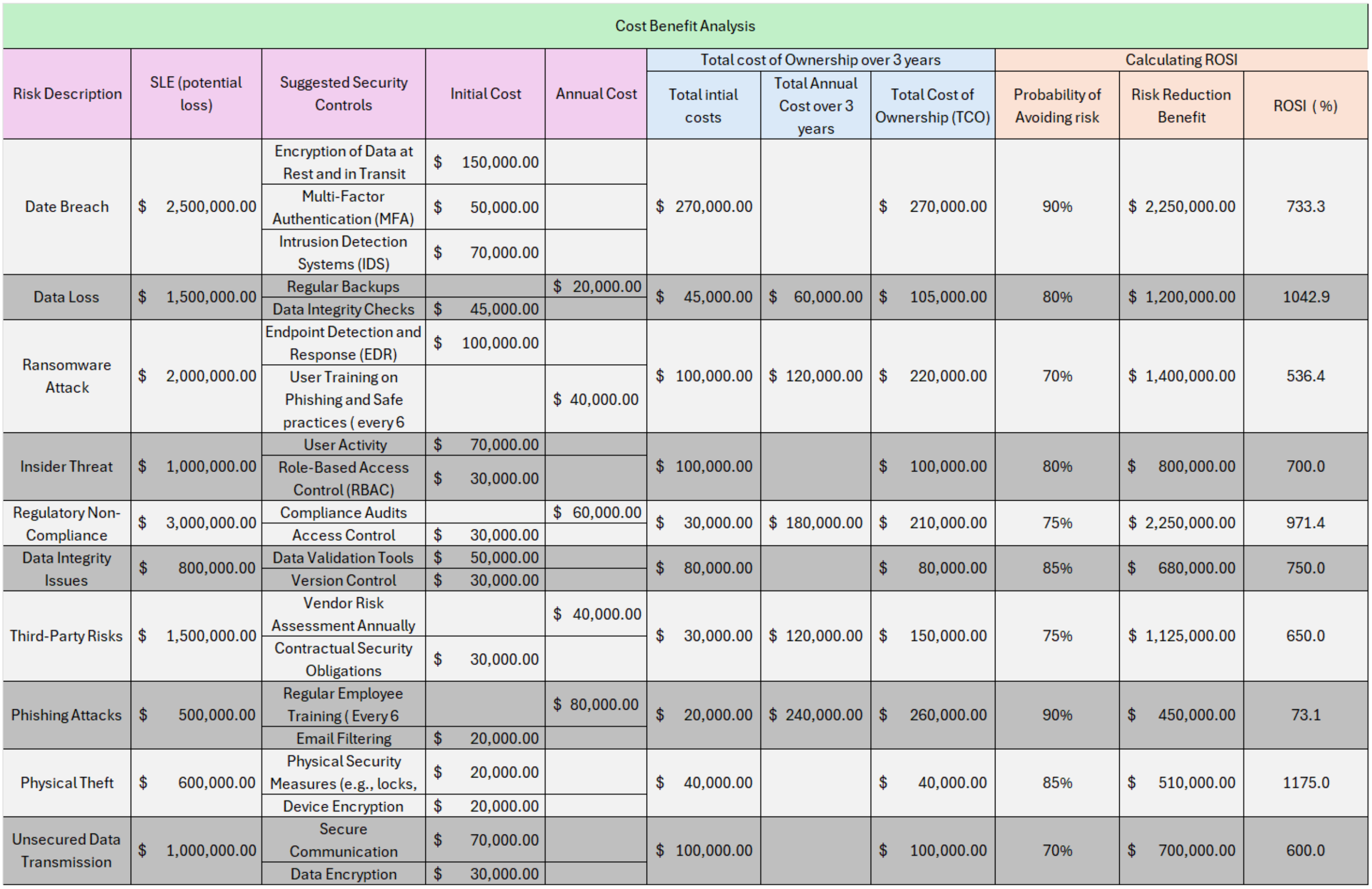
Note:

Priority 1-5: These represent the most critical controls and should be implemented immediately due to their high effectiveness and alignment with key risks.

Priority 6-10: These are important controls but can be scheduled after the implementation of higher-priority controls.

In our case, data breach is our main priority then data loss since data breach will have biggest impact on security control (The SANS Institute, 2021).

3.3 Cost-benefit analysis:



Cost Benefit Analysis										
					Total cost of Ownership over 3 years			Calculating ROSI		
Risk Description	SLE (potential loss)	Suggested Security Controls	Initial Cost	Annual Cost	Total intial costs	Total Annual Cost over 3 years	Total Cost of Ownership (TCO)	Probability of Avoiding risk	Risk Reduction Benefit	ROSI (%)
Date Breach	$ 2,500,000.00	Encryption of Data at Rest and in Transit	$ 150,000.00		$ 270,000.00		$ 270,000.00	90%	$ 2,250,000.00	733.3
		Multi-Factor Authentication (MFA)	$ 50,000.00							
		Intrusion Detection Systems (IDS)	$ 70,000.00							
Data Loss	$ 1,500,000.00	Regular Backups		$ 20,000.00	$ 45,000.00	$ 60,000.00	$ 105,000.00	80%	$ 1,200,000.00	1042.9
		Data Integrity Checks	$ 45,000.00							
Ransomware Attack	$ 2,000,000.00	Endpoint Detection and Response (EDR)	$ 100,000.00		$ 100,000.00	$ 120,000.00	$ 220,000.00	70%	$ 1,400,000.00	536.4
		User Training on Phishing and Safe practices (every 6		$ 40,000.00						
Insider Threat	$ 1,000,000.00	User Activity	$ 70,000.00		$ 100,000.00		$ 100,000.00	80%	$ 800,000.00	700.0
		Role-Based Access Control (RBAC)	$ 30,000.00							
Regulatory Non-Compliance	$ 3,000,000.00	Compliance Audits		$ 60,000.00	$ 30,000.00	$ 180,000.00	$ 210,000.00	75%	$ 2,250,000.00	971.4
		Access Control	$ 30,000.00							
Data Integrity Issues	$ 800,000.00	Data Validation Tools	$ 50,000.00		$ 80,000.00		$ 80,000.00	85%	$ 680,000.00	750.0
		Version Control	$ 30,000.00							
Third-Party Risks	$ 1,500,000.00	Vendor Risk Assessment Annually		$ 40,000.00	$ 30,000.00	$ 120,000.00	$ 150,000.00	75%	$ 1,125,000.00	650.0
		Contractual Security Obligations	$ 30,000.00							
Phishing Attacks	$ 500,000.00	Regular Employee Training (Every 6		$ 80,000.00	$ 20,000.00	$ 240,000.00	$ 260,000.00	90%	$ 450,000.00	73.1
		Email Filtering	$ 20,000.00							
Physical Theft	$ 600,000.00	Physical Security Measures (e.g., locks,	$ 20,000.00		$ 40,000.00		$ 40,000.00	85%	$ 510,000.00	1175.0
		Device Encryption	$ 20,000.00							
Unsecured Data Transmission	$ 1,000,000.00	Secure Communication	$ 70,000.00		$ 100,000.00		$ 100,000.00	70%	$ 700,000.00	600.0
		Data Encryption	$ 30,000.00							

Ransomware attack will be used as an example for ROSI calculation (National Institute of Standards and Technology [NIST], 2018) (Center for Internet Security, 2020) (United States Government Accountability Office, 2021).

Potential loss from ransomware attack: $ 2,000,000

Suggested Security Controls:	**Initial Costs:**
1. Endpoint Detection and Response (EDR)	$ 100,000
2. User Training on Phishing and Safe practice (Every 6 months)	Annual cost: $ 40,000

Total cost of Ownership over 3 years

Total Initial Costs = $ 100,000

Total Annual Costs = $ 40,000

$$TCO = Total\ Inital\ cost + (Total\ Annual\ Cost\ \times 3) = \$100{,}00 + \$120000 = \$\ 220{,}000$$

Return on Security Investment (ROSI)

Assumption for probability of ransomware attack is 70% (after implementing controls)

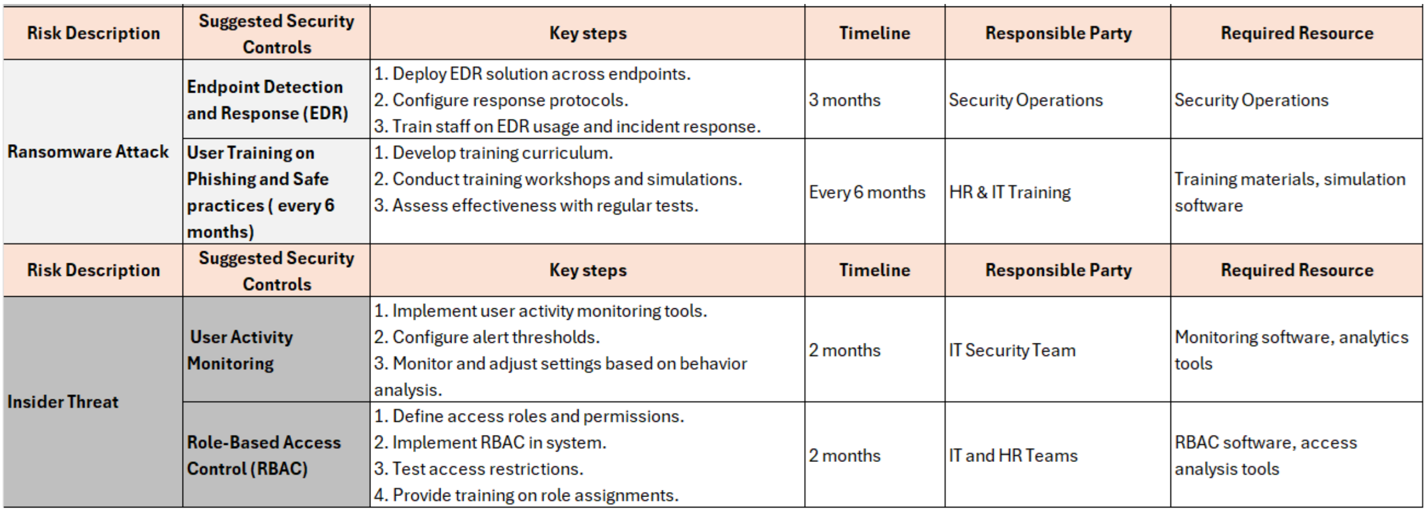
Risk Reduction benefit = $\$\ 2{,}000{,}000\ \times 0.7 = \$\ 1{,}400{,}000$

$$ROSI\ = \left(\frac{(Risk\ Reduction\ benefit - TCO)}{TCO}\right) \times 100$$

$$ROSI\ = \left(\frac{(\$1{,}400{,}000 - \$220{,}000)}{220{,}000}\right) \times 100 = 536.4\ \%$$

3.4 Implementation Plan:

The Suggested security controls from ransomware attack, and insider Threat will be used as example for implementation plan.

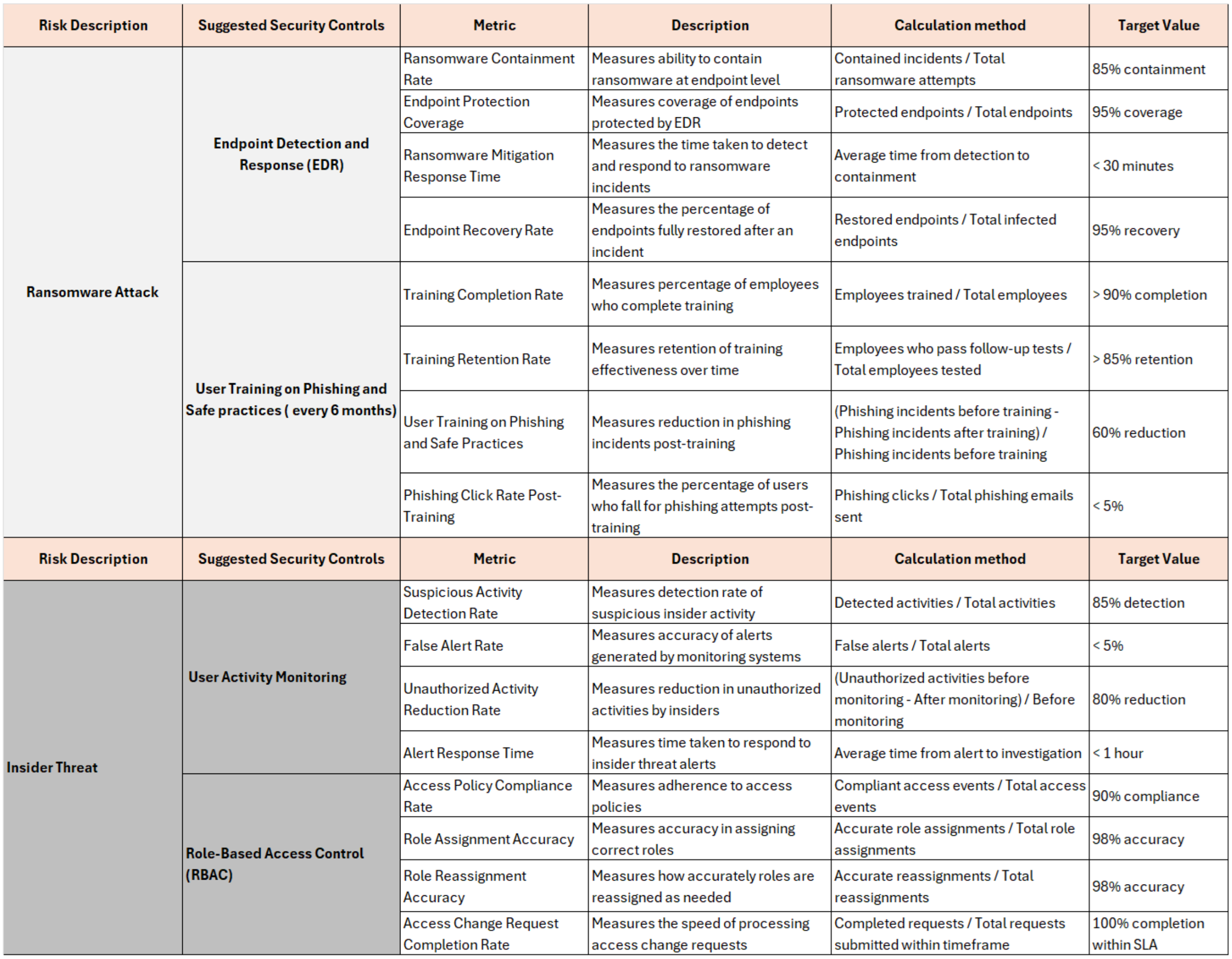


Risk Description	Suggested Security Controls	Key steps	Timeline	Responsible Party	Required Resource
Ransomware Attack	Endpoint Detection and Response (EDR)	1. Deploy EDR solution across endpoints. 2. Configure response protocols. 3. Train staff on EDR usage and incident response.	3 months	Security Operations	Security Operations
	User Training on Phishing and Safe practices (every 6 months)	1. Develop training curriculum. 2. Conduct training workshops and simulations. 3. Assess effectiveness with regular tests.	Every 6 months	HR & IT Training	Training materials, simulation software
Risk Description	Suggested Security Controls	Key steps	Timeline	Responsible Party	Required Resource
Insider Threat	User Activity Monitoring	1. Implement user activity monitoring tools. 2. Configure alert thresholds. 3. Monitor and adjust settings based on behavior analysis.	2 months	IT Security Team	Monitoring software, analytics tools
	Role-Based Access Control (RBAC)	1. Define access roles and permissions. 2. Implement RBAC in system. 3. Test access restrictions. 4. Provide training on role assignments.	2 months	IT and HR Teams	RBAC software, access analysis tools

The table provides an implementation plan for mitigating Ransomware Attacks and Insider Threats through selected security controls.

***** Please see Appendix B for Implementation plan for all security options*****

3.5 Cost-effective Security Metrics:



Risk Description	Suggested Security Controls	Metric	Description	Calculation method	Target Value
Ransomware Attack	Endpoint Detection and Response (EDR)	Ransomware Containment Rate	Measures ability to contain ransomware at endpoint level	Contained incidents / Total ransomware attempts	85% containment
		Endpoint Protection Coverage	Measures coverage of endpoints protected by EDR	Protected endpoints / Total endpoints	95% coverage
		Ransomware Mitigation Response Time	Measures the time taken to detect and respond to ransomware incidents	Average time from detection to containment	< 30 minutes
		Endpoint Recovery Rate	Measures the percentage of endpoints fully restored after an incident	Restored endpoints / Total infected endpoints	95% recovery
	User Training on Phishing and Safe practices (every 6 months)	Training Completion Rate	Measures percentage of employees who complete training	Employees trained / Total employees	> 90% completion
		Training Retention Rate	Measures retention of training effectiveness over time	Employees who pass follow-up tests / Total employees tested	> 85% retention
		User Training on Phishing and Safe Practices	Measures reduction in phishing incidents post-training	(Phishing incidents before training - Phishing incidents after training) / Phishing incidents before training	60% reduction
		Phishing Click Rate Post-Training	Measures the percentage of users who fall for phishing attempts post-training	Phishing clicks / Total phishing emails sent	< 5%
Risk Description	**Suggested Security Controls**	**Metric**	**Description**	**Calculation method**	**Target Value**
Insider Threat	User Activity Monitoring	Suspicious Activity Detection Rate	Measures detection rate of suspicious insider activity	Detected activities / Total activities	85% detection
		False Alert Rate	Measures accuracy of alerts generated by monitoring systems	False alerts / Total alerts	< 5%
		Unauthorized Activity Reduction Rate	Measures reduction in unauthorized activities by insiders	(Unauthorized activities before monitoring - After monitoring) / Before monitoring	80% reduction
		Alert Response Time	Measures time taken to respond to insider threat alerts	Average time from alert to investigation	< 1 hour
	Role-Based Access Control (RBAC)	Access Policy Compliance Rate	Measures adherence to access policies	Compliant access events / Total access events	90% compliance
		Role Assignment Accuracy	Measures accuracy in assigning correct roles	Accurate role assignments / Total role assignments	98% accuracy
		Role Reassignment Accuracy	Measures how accurately roles are reassigned as needed	Accurate reassignments / Total reassignments	98% accuracy
		Access Change Request Completion Rate	Measures the speed of processing access change requests	Completed requests / Total requests submitted within timeframe	100% completion within SLA

***** Please see Appendix C for Cost Effective Security Metrics for all security options*****

Conclusion

This cybersecurity risk management program provides a comprehensive framework for SolarWinds Corporation to protect its critical assets and mitigate cyber risks effectively. By systematically evaluating asset sensitivity, implementing prioritized security controls, and establishing continuous monitoring and periodic risk assessments, SolarWinds can strengthen its defenses against potential threats. This structured approach ensures that resources are allocated efficiently, enhancing both the security posture and resilience of SolarWinds in an evolving threat landscape.

Reference

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 8*, 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002

Cardenas, A. A., Manadhata, P. K., & Rajan, S. P. (2013). Big data analytics for security. *IEEE Security & Privacy, 11*(6), 74-76. https://doi.org/10.1109/MSP.2013.138

Center for Internet Security. (2020). *CIS Controls Version 8*. https://www.cisecurity.org/controls/ (accessed October 15, 2024).

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*(1), 33-56. https://doi.org/10.3233/JCS-2009-0390

Heiser, J., & Nicolett, M. (2020). Understanding and managing security risks in cloud computing. *Gartner Report*. https://www.gartner.com (accessed October 10, 2024).

Institute of Risk Management. (2018). *Cyber Risk Management: A Boardroom Perspective*. https://www.theirm.org (accessed October 22, 2024).

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. https://doi.org/10.6028/NIST.CSWP.04162018

NIST Special Publication 800-30. (2012). *Guide for Conducting Risk Assessments*. https://doi.org/10.6028/NIST.SP.800-30r1

Radvanovsky, R., & McDougall, J. (2018). *Critical Infrastructure: Homeland Security and Emergency Preparedness*. CRC Press.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company.

Shackleford, D. (2019). *Continuous Security Monitoring: Cybersecurity Controls for Advanced Threat Detection and Prevention*. SANS Institute. https://www.sans.org (accessed October 18, 2024).

SolarWinds Corporation. (2021). *SolarWinds Cyber Incident Response Report*. SolarWinds. https://www.solarwinds.com (accessed October 12, 2024).

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI): A practical quantitative model. *Journal of Research and Practice in Information Technology, 38*(1), 45-56. https://doi.org/10.5555/1234567.1234568

The SANS Institute. (2021). *Top 20 Critical Security Controls for Effective Cyber Defense*. https://www.sans.org (accessed October 20, 2024).

United States Government Accountability Office. (2021). *Critical Infrastructure Protection: Progress and Challenges*. https://www.gao.gov (accessed October 5, 2024).

Appendix

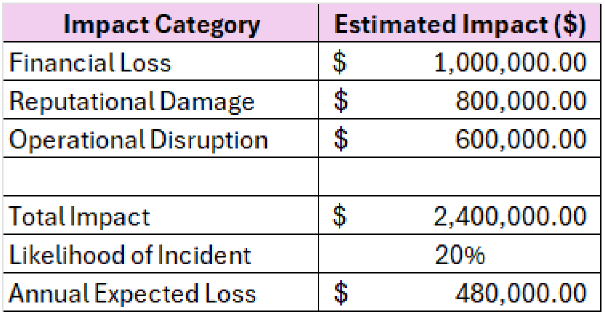
Appendix A

Business Impact Analysis – Physical Assets

2. Networking Equipment

Assumptions: Networking equipment is essential for connectivity and affects all systems.

Impact Categories: Financial Loss, Reputational Damage, Operational Disruption.



Impact Category	Estimated Impact ($)
Financial Loss	$ 1,000,000.00
Reputational Damage	$ 800,000.00
Operational Disruption	$ 600,000.00
Total Impact	$ 2,400,000.00
Likelihood of Incident	20%
Annual Expected Loss	$ 480,000.00

Estimated Impact Values:

- Financial Loss: $1,000,000 (including service restoration and replacement costs).
- Reputational Damage: $800,000 (customer dissatisfaction due to prolonged downtime).
- Operational Disruption: $600,000 (lost productivity and reconfiguration).

Likelihood of Incident: 20% (1 in 5 chance of significant network disruption in a year)

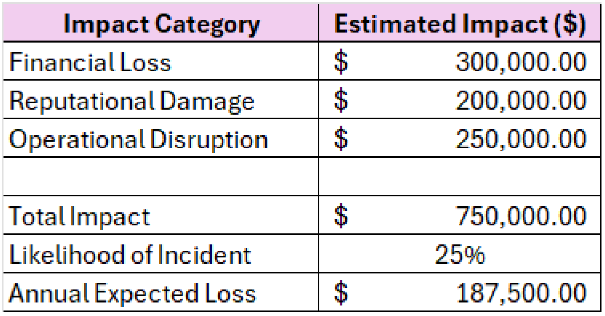
Impact Calculation:

- **Total Impact** = Financial Loss + Reputational Damage + Operational Disruption
- **Total Impact** = $1,000,000 + $800,000 + $600,000 = $2,400,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident
- **Annual Expected Loss** = $2,400,000 × 0.20 = $480,000

3. Endpoint Devices



Impact Category	Estimated Impact ($)
Financial Loss	$ 300,000.00
Reputational Damage	$ 200,000.00
Operational Disruption	$ 250,000.00
Total Impact	$ 750,000.00
Likelihood of Incident	25%
Annual Expected Loss	$ 187,500.00

Assumptions: Endpoint devices are primarily used for employee access and can be vulnerable to theft or unauthorized access.

Impact Categories: Financial Loss, Reputational Damage, Operational Disruption.

Estimated Impact Values:

- Financial Loss: $300,000 (includes device replacement and potential data recovery costs)
- Reputational Damage: $200,000 (limited impact on customer trust if data leakage occurs)
- Operational Disruption: $250,000 (impact on productivity and IT support)

Likelihood of Incident: 25% (1 in 4 chance of endpoint compromise in a year)

Impact Calculation:

- **Total Impact** = Financial Loss + Reputational Damage + Operational Disruption
- **Total Impact** = $300,000 + $200,000 + $250,000 = $750,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident
- **Annual Expected Loss** = $750,000 × 0.25 = $187,500

Business Impact Analysis – Digital Assets

2. SIEM Tools

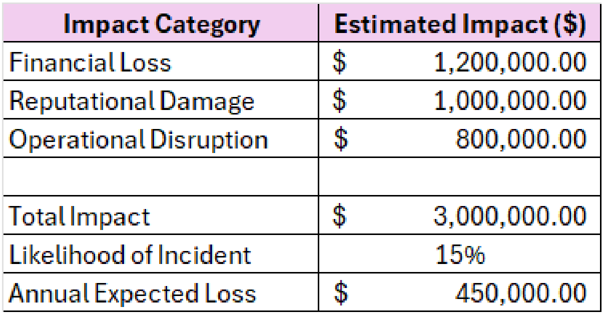
Assumptions: Essential for threat detection and response; failure could expose systems to vulnerabilities.

Impact Categories: Financial Loss, Reputational Damage, Operational Disruption.

Estimated Impact Values:

- Financial Loss: $1,200,000 (loss due to prolonged exposure to threats)

- Reputational Damage: $1,000,000 (customer trust affected due to potential data breaches)
- Operational Disruption: $800,000 (increased remediation costs and response delays)



Impact Category	Estimated Impact ($)
Financial Loss	$ 1,200,000.00
Reputational Damage	$ 1,000,000.00
Operational Disruption	$ 800,000.00
Total Impact	$ 3,000,000.00
Likelihood of Incident	15%
Annual Expected Loss	$ 450,000.00

Likelihood of Incident: 15% (1 in 6.7 chance of failure or compromise annually)

Impact Calculation:

- **Total Impact** = Financial Loss + Reputational Damage + Operational Disruption
- **Total Impact** = $1,200,000 + $1,000,000 + $800,000 = $3,000,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident
- **Annual Expected Loss** = $3,000,000 × 0.15 = $450,000

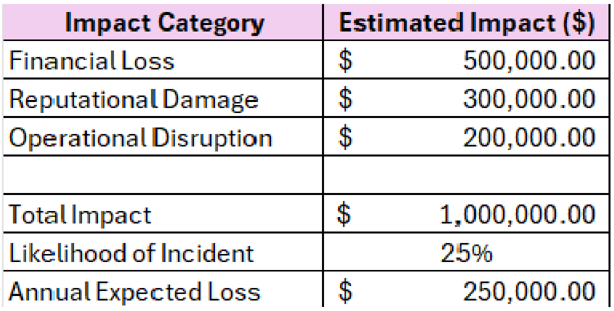
3. Antivirus Software

Assumptions: Provides a layer of defense against malware; not critical but important for preventing infections.

Impact Categories: Financial Loss, Reputational Damage, Operational Disruption.

Estimated Impact Values:

- Financial Loss: $500,000 (cost of potential malware cleanup and recovery)
- Reputational Damage: $300,000 (limited reputational impact if only a minor infection)
- Operational Disruption: $200,000 (minor impact on operations due to infection)



Impact Category	Estimated Impact ($)
Financial Loss	$ 500,000.00
Reputational Damage	$ 300,000.00
Operational Disruption	$ 200,000.00
Total Impact	$ 1,000,000.00
Likelihood of Incident	25%
Annual Expected Loss	$ 250,000.00

Likelihood of Incident: 25% (1 in 4 chance of infection bypassing antivirus in a year)

Impact Calculation:

- **Total Impact** = Financial Loss + Reputational Damage + Operational Disruption
- **Total Impact** = $500,000 + $300,000 + $200,000 = $1,000,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident
- **Annual Expected Loss** = $1,000,000 × 0.25 = $250,000

Customer Records

Assumptions: Contains sensitive client data; compromise could lead to regulatory issues and heavy fines.

Impact Categories: Financial Loss, Reputational Damage, Regulatory Penalties.

Estimated Impact Values:

- Financial Loss: $2,500,000 (potential data breach fines and compensation to clients)
- Reputational Damage: $4,000,000 (significant trust impact and potential client loss)
- Regulatory Penalties: $3,000,000 (GDPR or other regulatory fines)

Likelihood of Incident: 10% (1 in 10 chance of data breach in a year)

Impact Calculation:

- **Total Impact** = Financial Loss + Reputational Damage + Regulatory Penalties
- **Total Impact** = $2,500,000 + $4,000,000 + $3,000,000 = $9,500,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident
- **Annual Expected Loss** = $9,500,000 × 0.10 = $950,000

Configuration Files

Assumptions: Stores system settings; compromised files could lead to system downtime and configuration errors.

Impact Categories: Financial Loss, Operational Disruption.

Estimated Impact Values:

- Financial Loss: $400,000 (costs for reconfiguration and troubleshooting)

- Operational Disruption: $ $600,000 (downtime impact on productivity and service availability)

Likelihood of Incident: 20% (1 in 5 chance of configuration error or corruption in a year)

Impact Calculation:

- **Total Impact** = Financial Loss + Operational Disruption
- **Total Impact** = $400,000 + $600,000 = $1,000,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident
- **Annual Expected Loss** = $1,000,000 × 0.20 = $200,000

Intellectual Property

Assumptions: Includes proprietary source code, product designs, and trade secrets that provide a competitive advantage.

Impact Categories: Financial Loss, Reputational Damage, Competitive Disadvantage.

Estimated Impact Values:

- Financial Loss: $2,500,000 (loss due to intellectual property theft and potential legal expenses)
- Reputational Damage: $1,500,000 (customer trust affected if intellectual property is compromised)
- Competitive Disadvantage: $3,000,000 (reduced market position due to leaked proprietary data)

Likelihood of Incident: 8% (1 in 12.5 chance of intellectual property theft in a year)

Impact Calculation:

- **Total Impact** = Financial Loss + Reputational Damage + Competitive Disadvantage
- **Total Impact** = $2,500,000 + $1,500,000 + $3,000,000 = $7,000,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident
- **Annual Expected Loss** = $7,000,000 × 0.08 = $560,000

Threat intelligence

Assumptions: Includes data on emerging threats, vulnerabilities, and potential attack vectors; vital for proactive defense.

Impact Categories: Operational Disruption, Competitive Disadvantage, Reputational Damage.

Estimated Impact Values:

- Reputational Damage: $400,000 (clients' perception of inadequate security if threat data is exposed)
- Competitive Disadvantage: $500,000 (decreased ability to respond to industry threats)
- Operational Disruption: $600,000 (increased risk of incidents due to delayed threat responses)

Likelihood of Incident: 12% (1 in 8.3 chance of compromise in a year)

Impact Calculation:

- **Total Impact** = Reputational Damage + Competitive Disadvantage + Operational Disruption
- **Total Impact** = $400,000 + $500,000 + $600,000 = $1,500,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident
- **Annual Expected Loss** = $750,000 × 0.25 = $187,500

Internal Documentation

Assumptions: Includes operational manuals, policies, and protocols; primarily used for internal processes.

Impact Categories: Operational Disruption, Compliance Issues.

Estimated Impact Values:

- Operational Disruption: $200,000 (impact on internal workflows due to loss or compromise of internal procedures)
- Compliance Issues: $150,000 (potential penalties if loss leads to non-compliance with internal audits)

Likelihood of Incident: 10% (1 in 10 chance of documentation compromise in a year)

Impact Calculation:

- **Total Impact** = Operational Disruption + Compliance Issues
- **Total Impact** = $200,000 + $150,000 = $350,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident
- **Annual Expected Loss** = $350,000 × 0.10 = $35,000

Business Impact Analysis – Human Assets

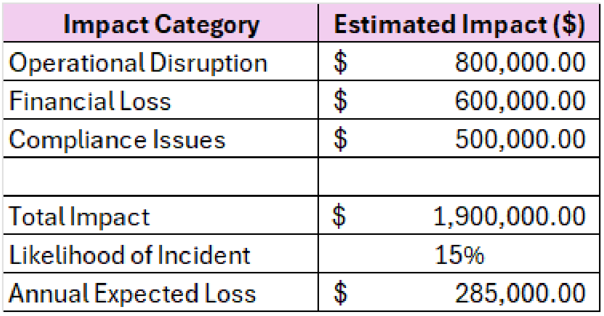
2.Third-Party Vendors

Assumptions: Vendors provide specialized services, including software development, security assessments, and consulting.

Impact Categories: Operational Disruption, Financial Loss, Compliance Issues.

Estimated Impact Values:

- Operational Disruption: $800,000 (dependency on vendor services could lead to delays if they fail to deliver)
- Financial Loss: $600,000 (cost of finding new vendors or fulfilling SLAs due to vendor issues)
- Compliance Issues: $500,000 (potential legal and regulatory penalties if vendor issues lead to security lapses)



Impact Category	Estimated Impact ($)
Operational Disruption	$ 800,000.00
Financial Loss	$ 600,000.00
Compliance Issues	$ 500,000.00
Total Impact	$ 1,900,000.00
Likelihood of Incident	15%
Annual Expected Loss	$ 285,000.00

Likelihood of Incident: 15% (1 in 6.7 chance of vendor-related disruptions in a year)

Impact Calculation:

- **Total Impact** = Operational Disruption + Financial Loss + Compliance Issues
- **Total Impact** = $800,000 + $600,000 + $500,000 = $1,900,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident
- **Annual Expected Loss** = $1,900,000 × 0.15 = $285,000

3.Contractors

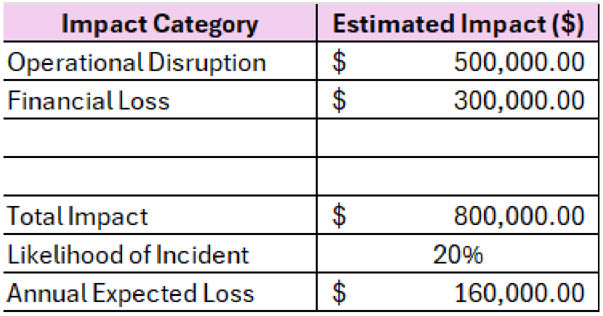
Assumptions: Contractors are temporary staff brought in for specific tasks or projects.

Impact Categories: Operational Disruption, Financial Loss.

Estimated Impact Values:

- Operational Disruption: $500,000 (delay or disruption in projects if contractors are unavailable or compromised)
- Financial Loss: $300,000 (costs associated with rehiring and onboarding new contractors)

Likelihood of Incident: 20% (1 in 5 chances of disruption due to contractor unavailability or issues in a year)



Impact Category	Estimated Impact ($)
Operational Disruption	$ 500,000.00
Financial Loss	$ 300,000.00
Total Impact	$ 800,000.00
Likelihood of Incident	20%
Annual Expected Loss	$ 160,000.00

Impact Calculation:

- **Total Impact** = Operational Disruption + Financial Loss
- **Total Impact** = $500,000 + $300,000 = $800,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident
- **Annual Expected Loss** = $800,000 × 0.20 = $160,000

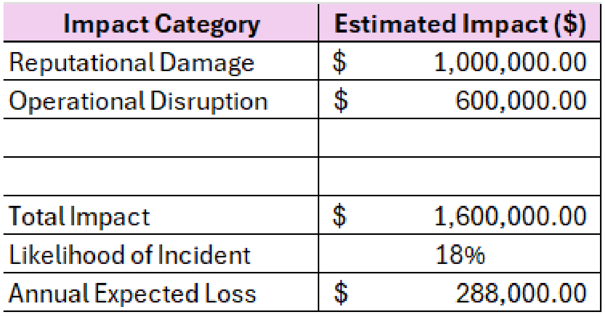
4. Support Teams

Assumptions: Support teams are responsible for customer service and addressing client issues, impacting client satisfaction directly.

Impact Categories: Reputational Damage, Operational Disruption.

Estimated Impact Values:

- Reputational Damage: $1,000,000 (significant impact on customer trust if support is unavailable)
- Operational Disruption: $600,000 (lost productivity and potential service delays impacting client interactions)



Impact Category	Estimated Impact ($)
Reputational Damage	$ 1,000,000.00
Operational Disruption	$ 600,000.00
Total Impact	$ 1,600,000.00
Likelihood of Incident	18%
Annual Expected Loss	$ 288,000.00

Likelihood of Incident: 18% (1 in 5.5 chance of support team unavailability or compromise in a year)

Impact Calculation:

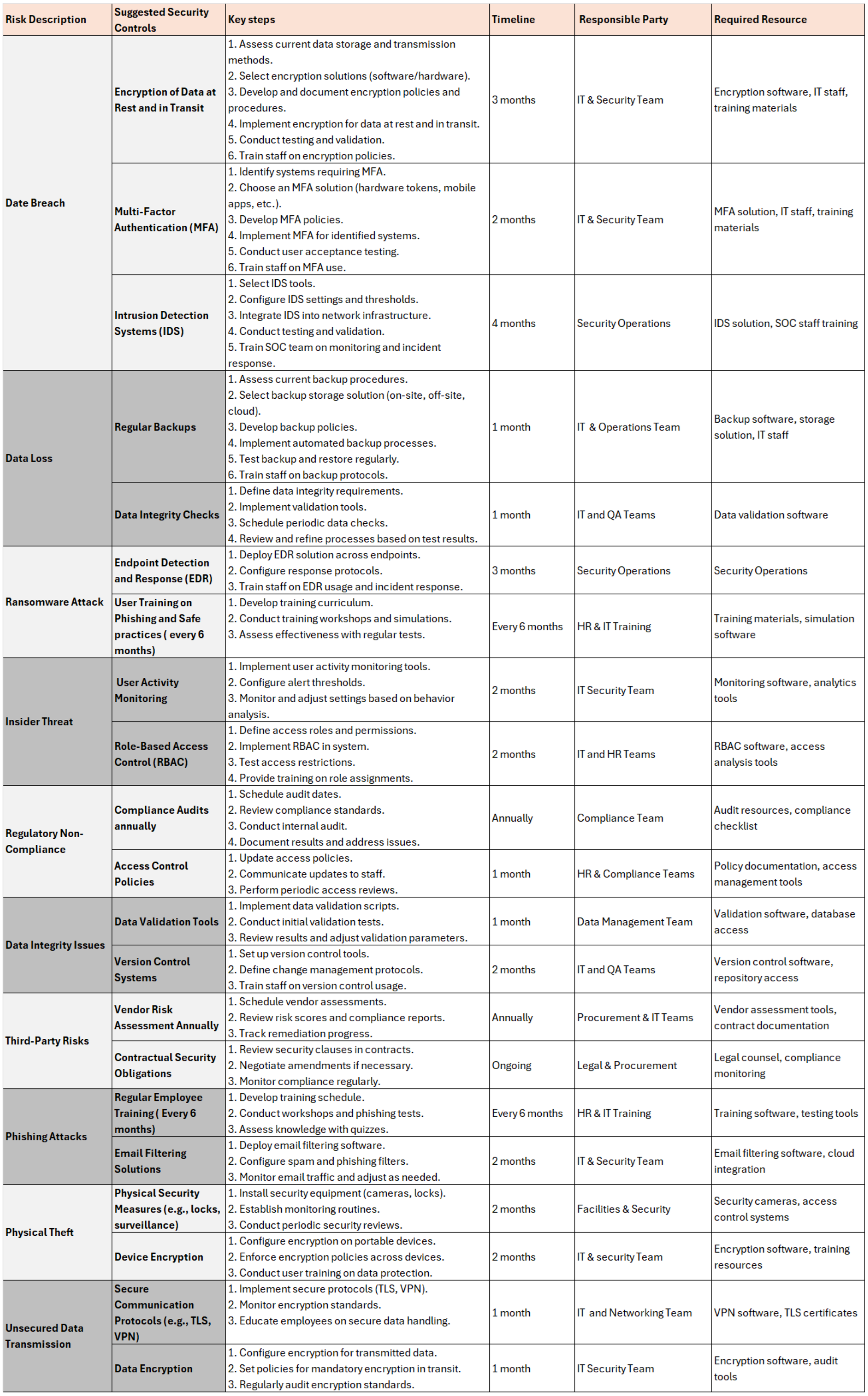
- **Total Impact** = Reputational Damage + Operational Disruption
- **Total Impact** = $1,000,000 + $600,000 = $1,600,000

Annual Expected Loss Calculation:

- **Annual Expected Loss** = Total Impact × Likelihood of Incident

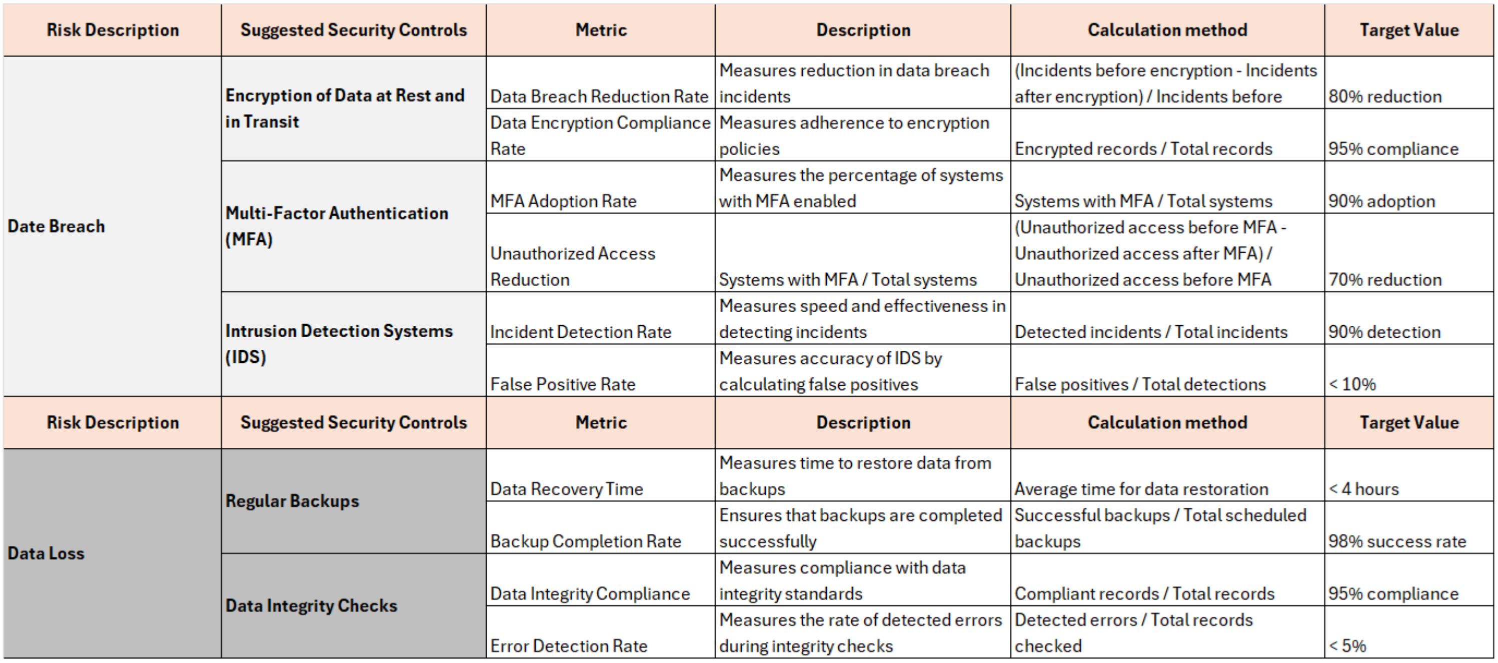
Annual Expected Loss = $1,600,000 × 0.18 = $288,000

Appendix B

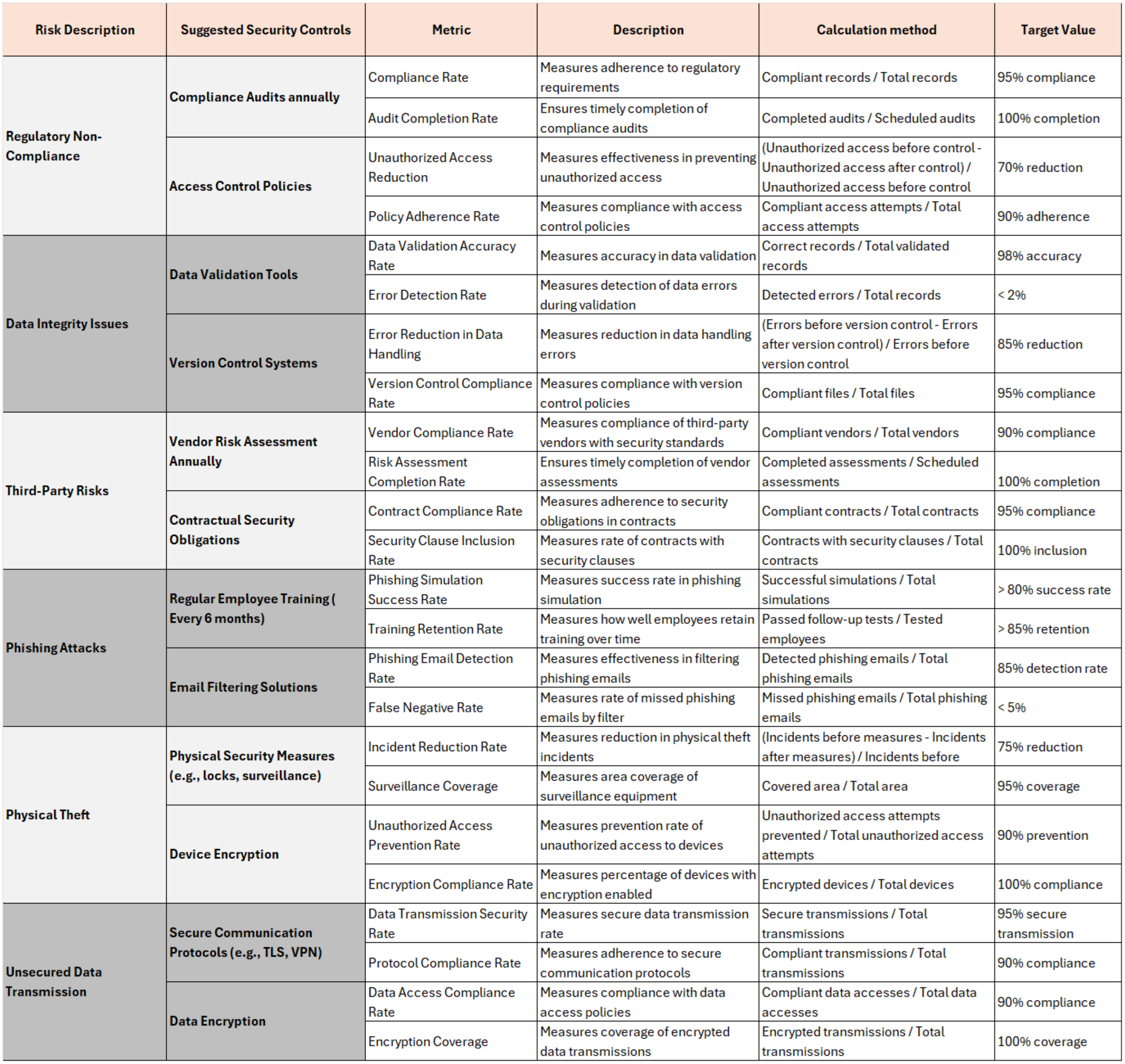


Risk Description	Suggested Security Controls	Key steps	Timeline	Responsible Party	Required Resource
Date Breach	Encryption of Data at Rest and in Transit	1. Assess current data storage and transmission methods. 2. Select encryption solutions (software/hardware). 3. Develop and document encryption policies and procedures. 4. Implement encryption for data at rest and in transit. 5. Conduct testing and validation. 6. Train staff on encryption policies.	3 months	IT & Security Team	Encryption software, IT staff, training materials
	Multi-Factor Authentication (MFA)	1. Identify systems requiring MFA. 2. Choose an MFA solution (hardware tokens, mobile apps, etc.). 3. Develop MFA policies. 4. Implement MFA for identified systems. 5. Conduct user acceptance testing. 6. Train staff on MFA use.	2 months	IT & Security Team	MFA solution, IT staff, training materials
	Intrusion Detection Systems (IDS)	1. Select IDS tools. 2. Configure IDS settings and thresholds. 3. Integrate IDS into network infrastructure. 4. Conduct testing and validation. 5. Train SOC team on monitoring and incident response.	4 months	Security Operations	IDS solution, SOC staff training
Data Loss	Regular Backups	1. Assess current backup procedures. 2. Select backup storage solution (on-site, off-site, cloud). 3. Develop backup policies. 4. Implement automated backup processes. 5. Test backup and restore regularly. 6. Train staff on backup protocols.	1 month	IT & Operations Team	Backup software, storage solution, IT staff
	Data Integrity Checks	1. Define data integrity requirements. 2. Implement validation tools. 3. Schedule periodic data checks. 4. Review and refine processes based on test results.	1 month	IT and QA Teams	Data validation software
Ransomware Attack	Endpoint Detection and Response (EDR)	1. Deploy EDR solution across endpoints. 2. Configure response protocols. 3. Train staff on EDR usage and incident response.	3 months	Security Operations	Security Operations
	User Training on Phishing and Safe practices (every 6 months)	1. Develop training curriculum. 2. Conduct training workshops and simulations. 3. Assess effectiveness with regular tests.	Every 6 months	HR & IT Training	Training materials, simulation software
Insider Threat	User Activity Monitoring	1. Implement user activity monitoring tools. 2. Configure alert thresholds. 3. Monitor and adjust settings based on behavior analysis.	2 months	IT Security Team	Monitoring software, analytics tools
	Role-Based Access Control (RBAC)	1. Define access roles and permissions. 2. Implement RBAC in system. 3. Test access restrictions. 4. Provide training on role assignments.	2 months	IT and HR Teams	RBAC software, access analysis tools
Regulatory Non-Compliance	Compliance Audits annually	1. Schedule audit dates. 2. Review compliance standards. 3. Conduct internal audit. 4. Document results and address issues.	Annually	Compliance Team	Audit resources, compliance checklist
	Access Control Policies	1. Update access policies. 2. Communicate updates to staff. 3. Perform periodic access reviews.	1 month	HR & Compliance Teams	Policy documentation, access management tools
Data Integrity Issues	Data Validation Tools	1. Implement data validation scripts. 2. Conduct initial validation tests. 3. Review results and adjust validation parameters.	1 month	Data Management Team	Validation software, database access
	Version Control Systems	1. Set up version control tools. 2. Define change management protocols. 3. Train staff on version control usage.	2 months	IT and QA Teams	Version control software, repository access
Third-Party Risks	Vendor Risk Assessment Annually	1. Schedule vendor assessments. 2. Review risk scores and compliance reports. 3. Track remediation progress.	Annually	Procurement & IT Teams	Vendor assessment tools, contract documentation
	Contractual Security Obligations	1. Review security clauses in contracts. 2. Negotiate amendments if necessary. 3. Monitor compliance regularly.	Ongoing	Legal & Procurement	Legal counsel, compliance monitoring
Phishing Attacks	Regular Employee Training (Every 6 months)	1. Develop training schedule. 2. Conduct workshops and phishing tests. 3. Assess knowledge with quizzes.	Every 6 months	HR & IT Training	Training software, testing tools
	Email Filtering Solutions	1. Deploy email filtering software. 2. Configure spam and phishing filters. 3. Monitor email traffic and adjust as needed.	2 months	IT & Security Team	Email filtering software, cloud integration
Physical Theft	Physical Security Measures (e.g., locks, surveillance)	1. Install security equipment (cameras, locks). 2. Establish monitoring routines. 3. Conduct periodic security reviews.	2 months	Facilities & Security	Security cameras, access control systems
	Device Encryption	1. Configure encryption on portable devices. 2. Enforce encryption policies across devices. 3. Conduct user training on data protection.	2 months	IT & security Team	Encryption software, training resources
Unsecured Data Transmission	Secure Communication Protocols (e.g., TLS, VPN)	1. Implement secure protocols (TLS, VPN). 2. Monitor encryption standards. 3. Educate employees on secure data handling.	1 month	IT and Networking Team	VPN software, TLS certificates
	Data Encryption	1. Configure encryption for transmitted data. 2. Set policies for mandatory encryption in transit. 3. Regularly audit encryption standards.	1 month	IT Security Team	Encryption software, audit tools

Appendix C



Risk Description	Suggested Security Controls	Metric	Description	Calculation method	Target Value
Date Breach	Encryption of Data at Rest and in Transit	Data Breach Reduction Rate	Measures reduction in data breach incidents	(Incidents before encryption - Incidents after encryption) / Incidents before	80% reduction
		Data Encryption Compliance Rate	Measures adherence to encryption policies	Encrypted records / Total records	95% compliance
	Multi-Factor Authentication (MFA)	MFA Adoption Rate	Measures the percentage of systems with MFA enabled	Systems with MFA / Total systems	90% adoption
		Unauthorized Access Reduction	Systems with MFA / Total systems	(Unauthorized access before MFA - Unauthorized access after MFA) / Unauthorized access before MFA	70% reduction
	Intrusion Detection Systems (IDS)	Incident Detection Rate	Measures speed and effectiveness in detecting incidents	Detected incidents / Total incidents	90% detection
		False Positive Rate	Measures accuracy of IDS by calculating false positives	False positives / Total detections	< 10%
Risk Description	**Suggested Security Controls**	**Metric**	**Description**	**Calculation method**	**Target Value**
Data Loss	Regular Backups	Data Recovery Time	Measures time to restore data from backups	Average time for data restoration	< 4 hours
		Backup Completion Rate	Ensures that backups are completed successfully	Successful backups / Total scheduled backups	98% success rate
	Data Integrity Checks	Data Integrity Compliance	Measures compliance with data integrity standards	Compliant records / Total records	95% compliance
		Error Detection Rate	Measures the rate of detected errors during integrity checks	Detected errors / Total records checked	< 5%



Risk Description	Suggested Security Controls	Metric	Description	Calculation method	Target Value
Regulatory Non-Compliance	Compliance Audits annually	Compliance Rate	Measures adherence to regulatory requirements	Compliant records / Total records	95% compliance
		Audit Completion Rate	Ensures timely completion of compliance audits	Completed audits / Scheduled audits	100% completion
	Access Control Policies	Unauthorized Access Reduction	Measures effectiveness in preventing unauthorized access	(Unauthorized access before control - Unauthorized access after control) / Unauthorized access before control	70% reduction
		Policy Adherence Rate	Measures compliance with access control policies	Compliant access attempts / Total access attempts	90% adherence
Data Integrity Issues	Data Validation Tools	Data Validation Accuracy Rate	Measures accuracy in data validation	Correct records / Total validated records	98% accuracy
		Error Detection Rate	Measures detection of data errors during validation	Detected errors / Total records	< 2%
	Version Control Systems	Error Reduction in Data Handling	Measures reduction in data handling errors	(Errors before version control - Errors after version control) / Errors before version control	85% reduction
		Version Control Compliance Rate	Measures compliance with version control policies	Compliant files / Total files	95% compliance
Third-Party Risks	Vendor Risk Assessment Annually	Vendor Compliance Rate	Measures compliance of third-party vendors with security standards	Compliant vendors / Total vendors	90% compliance
		Risk Assessment Completion Rate	Ensures timely completion of vendor assessments	Completed assessments / Scheduled assessments	100% completion
	Contractual Security Obligations	Contract Compliance Rate	Measures adherence to security obligations in contracts	Compliant contracts / Total contracts	95% compliance
		Security Clause Inclusion Rate	Measures rate of contracts with security clauses	Contracts with security clauses / Total contracts	100% inclusion
Phishing Attacks	Regular Employee Training (Every 6 months)	Phishing Simulation Success Rate	Measures success rate in phishing simulation	Successful simulations / Total simulations	> 80% success rate
		Training Retention Rate	Measures how well employees retain training over time	Passed follow-up tests / Tested employees	> 85% retention
	Email Filtering Solutions	Phishing Email Detection Rate	Measures effectiveness in filtering phishing emails	Detected phishing emails / Total phishing emails	85% detection rate
		False Negative Rate	Measures rate of missed phishing emails by filter	Missed phishing emails / Total phishing emails	< 5%
Physical Theft	Physical Security Measures (e.g., locks, surveillance)	Incident Reduction Rate	Measures reduction in physical theft incidents	(Incidents before measures - Incidents after measures) / Incidents before	75% reduction
		Surveillance Coverage	Measures area coverage of surveillance equipment	Covered area / Total area	95% coverage
	Device Encryption	Unauthorized Access Prevention Rate	Measures prevention rate of unauthorized access to devices	Unauthorized access attempts prevented / Total unauthorized access attempts	90% prevention
		Encryption Compliance Rate	Measures percentage of devices with encryption enabled	Encrypted devices / Total devices	100% compliance
Unsecured Data Transmission	Secure Communication Protocols (e.g., TLS, VPN)	Data Transmission Security Rate	Measures secure data transmission rate	Secure transmissions / Total transmissions	95% secure transmission
		Protocol Compliance Rate	Measures adherence to secure communication protocols	Compliant transmissions / Total transmissions	90% compliance
	Data Encryption	Data Access Compliance Rate	Measures compliance with data access policies	Compliant data accesses / Total data accesses	90% compliance
		Encryption Coverage	Measures coverage of encrypted data transmissions	Encrypted transmissions / Total transmissions	100% coverage