

Risk Assessment Report

1. Executive Summary

This risk assessment exercise was conducted to evaluate the potential impact and likelihood of a ransomware attack scenario using Annualized Loss Expectancy (ALE) and a 5x5 risk matrix. The objective is to align with SANS risk assessment practices, providing a structured methodology for calculating financial impact and mapping it to qualitative risk levels.

2. Scope

The scope of this assessment covers a ransomware scenario where the Single Loss Expectancy (SLE) and Annualized Rate of Occurrence (ARO) are defined, followed by ALE calculation and placement within a risk matrix.

3. Methodology

1. Define SLE (Single Loss Expectancy).
2. Define ARO (Annualized Rate of Occurrence).
3. Calculate ALE (Annualized Loss Expectancy).
4. Map ALE values into a 5x5 risk matrix (Likelihood vs. Impact).

4. Calculations

The calculations for the ransomware scenario are as follows:

SLE = \$10,000 ,falls into the \$5k–\$20k = Moderate (3) impact category

ARO = 0.2 (once every 5 years) ,this corresponds to Unlikely (2) in most 5x5 risk matrices.

$ALE = SLE \times ARO$

$ALE = \$10,000 \times 0.2 = \$2,000$

5. Risk Matrix

The following 5x5 risk matrix was used to determine the severity of the ransomware threat. The impact values are categorized into ranges, while the likelihood ranges from Rare (1) to Almost Certain (5).

SLE CALCULATED: \$10,000						
ALE CALCULATED: \$2000						
ALE	Impact ↓ / Likelihood →	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain (5)
<\$1K	Insignificant (1)	Low	Low	Low	Low	Medium
\$1k–\$5k	Minor (2)	Low	Low	Medium	Medium	High
\$5k–\$20k	Moderate (3)	Low	Medium	Medium	High	High
\$20k–\$100k	Major (4)	Medium	Medium	High	High	Critical
>\$100k	Catastrophic (5)	Medium	High	High	Critical	Critical

Risk Matrix (Likelihood × Impact):

6. Scenario Placement

The calculated risk scenario (SLE = \$10,000, ALE = \$2,000) falls under the Moderate impact category with a likelihood between Unlikely to Possible. This positions the risk in the Medium Risk zone of the matrix.

7. Recommendations

1. Implement robust backup and recovery mechanisms to reduce SLE in case of ransomware.
2. Enhance security awareness training to lower the likelihood of successful ransomware infections.
3. Apply endpoint detection and response (EDR) solutions to identify and block ransomware early.
4. Regularly patch systems and monitor network traffic to reduce attack surface.