Starter Content Pack:
Outage of Critical Network Share by an External Actor via Ransomware Overview

Scenario at a Glance

- **Threat:** External Malicious Actor
- **Asset:** Critical Network Share
- **Effect:** Availability
- **Method:** Ransomware

Overview

The purpose of this analysis is to quantify the risk associated with an external malicious actor causing an outage of a critical network share via a ransomware attack.

This content pack contains this analysis because of the continued rise of ransomware attacks. According to the 2021 Verizon Data Breach Investigations Report (DBIR), ransomware cases have been on an upward trend since 2016 and now account for 5% of total incidents, with 7.8% of organizations attempting to download at least one piece of known ransomware last year. This scenario's asset is Critical Network Share (shared network drives) because it is generally easy to access, and therefore an easy target for propagating ransomware.

Key FAIR^{TM} Components

- **Threat Event Frequency (TEF):** The number of times per year an external actor successfully gains a network foothold with the intent to propagate ransomware. In other words, the frequency in which ransomware software is successfully downloaded onto an endpoint but has not yet been executed.
- **Vulnerability:** After an external actor gains a network foothold and successfully downloads ransomware onto an endpoint, this is the percentage of time ransomware is executed and propagates to infect the asset.

Data Sources

The RiskLens' Starter content pack comes prepopulated in the RiskLens platform with data, risk scenarios, and other content. Each risk scenario is fully populated with expert-estimated ranges and draws on RiskLens' experience, third-party content, and data helpers available in the Starter content pack in the catalog. All relevant data sources and assumptions are documented in the accompanying workshop rationale so you can be confident in the results.

The third-party sources referenced for this scenario include:

- 2020 Verizon Data Breach Investigations Report (DBIR)
- North America Industry Classifications System (NAICS)
- Coveware 2020 Ransomware Marketplace Report
- Veritas 2020 Ransomware Resiliency Report

Starter Content Pack Resources

This scenario uses estimates sourced from various data helpers for both frequency and magnitude workshop questions. When applicable, workshop questions using data helpers list the data helper and tier in the rationale. These data helpers are available via the Starter content pack in the catalog.

The Starter content pack data helpers used in this scenario include:

- Ransomware Detections on Workstations, per Year
- Ransomware Detections – Susceptibility to Asset Compromise
- Percentage of Employee Productivity Affected
- Loaded Hourly Employee Wage

You're encouraged to add the data helpers to your library to review their additional tiers and select the option best aligned with your organization. You can find additional information about this scenario's modeling and estimation within the workshop.

Starter Content Pack Purpose and Guidance

The RiskLens' Starter content pack enables efficient analysis of some of the most important and common risk scenarios that have been modeled using FAIR and RiskLens leading practices. The scenarios in this content pack are designed to provide structure and guidance for future analysis work, while also quantifying some of the most analyzed scenarios in the RiskLens' platform.