RiskLens

INDUSTRIAL COMPANY ASSESSES RANSOMWARE THREAT

ANALYSIS SCOPING

PURPOSE

Helping inform management about the significance of an emerging risk, such as ransomware

RISK SCENARIO DESCRIPTION

How much risk is associated with the growing frequency of ransomware – a type of software that encrypts files for ransom by cyber criminals.

ASSETS

Workstations and Mapped Share Drives

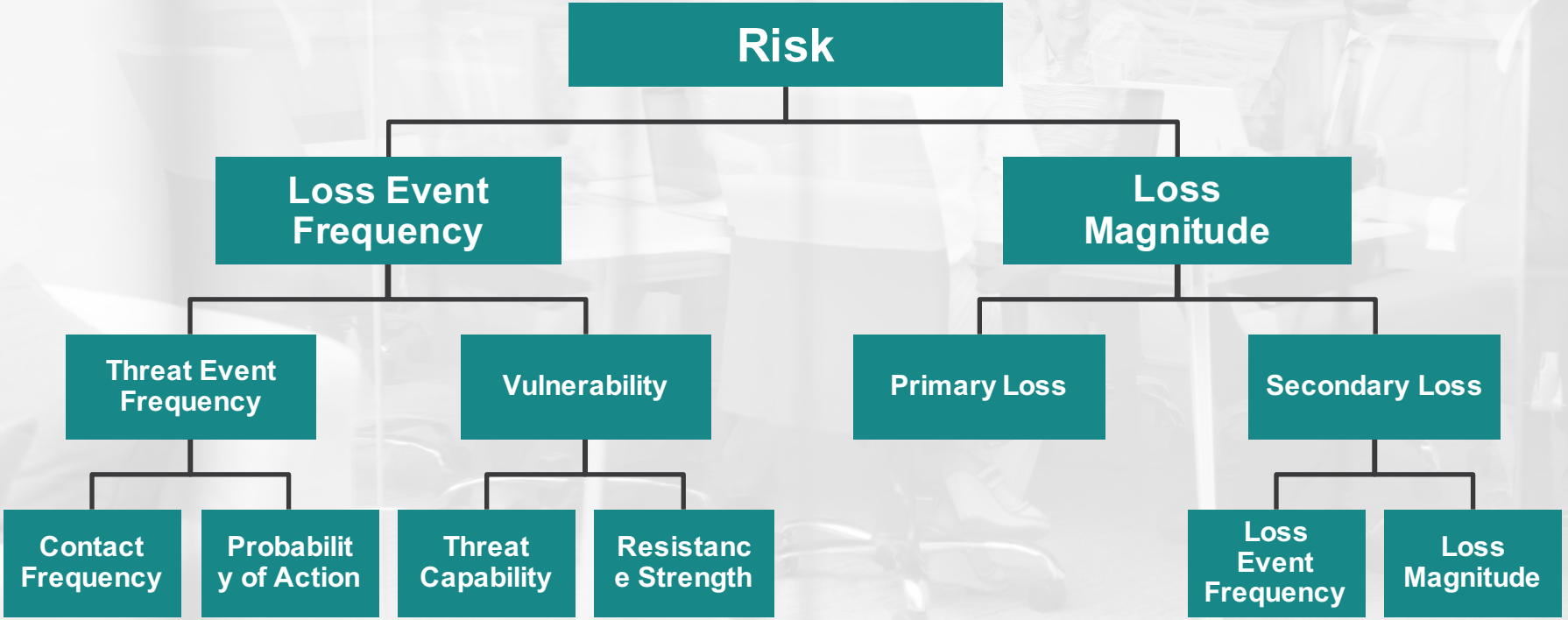
THREAT

Cyber Criminals

LOSS TYPE

Availability

RISK ANALYSIS MODEL



HOW OFTEN DO WE HAVE INCIDENTS?

RiskLens

NUMBER OF INCIDENTS

Asset	Minimum	Average	Maximum
Workstations	11	21	26
Shared Drives	1	3	5

- Ransomware targets workstations.
- When ransomware installs successfully on a workstation it may also encrypt any mounted shared drives the user has.

WHAT IS THE IMPACT PER EVENT?

RiskLens

IMPACT PER EVENT

Infection of	Minimum	Average	Maximum
Workstations	$300	**$1,000**	$2,000
Shared Drives	$31,000	**$640,000**	$2.1M

The impact will vary based on:

- The specific employee affected
- How much of operational productivity is affected
- Whether backups operated as expected and restoration of files is efficient

WHAT IS THE RISK OF RANSOMWARE?

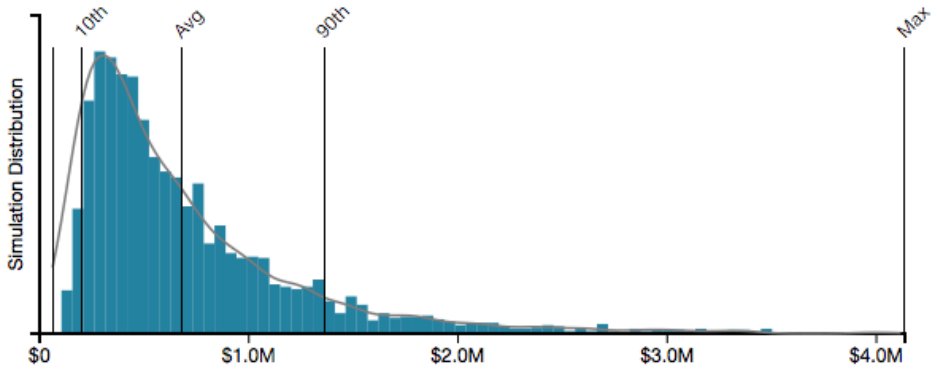
RiskLens

RESULT OF THE QUANTIFIED RISK ANALYSIS

Aggregate Loss Exposure

The aggregation of all independently analyzed risk scenarios.

Maximum	$4.1M
90th %	$1.4M
Average	$678K
10th %	$202K
Minimum	$62K



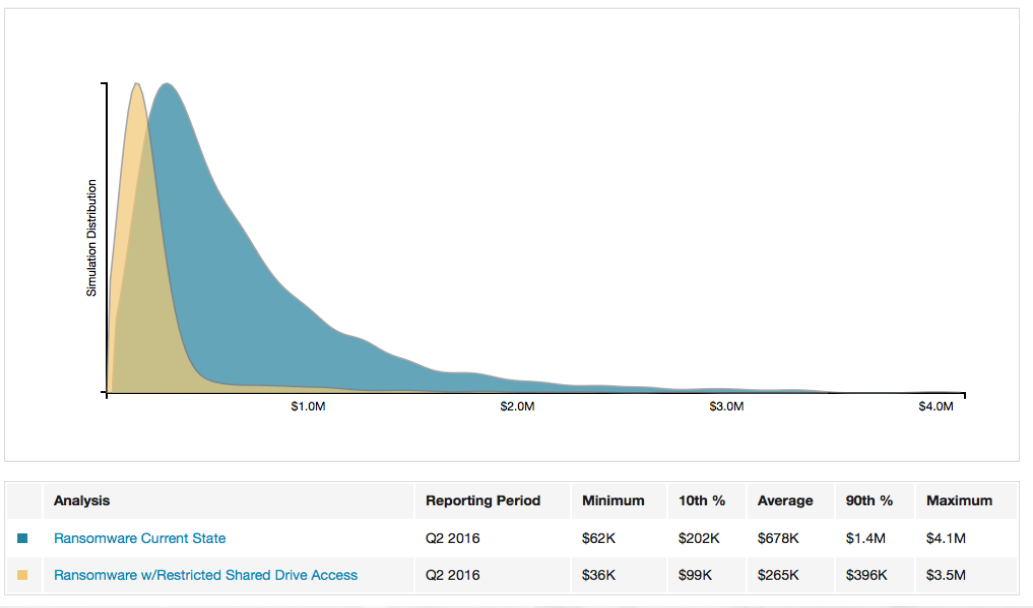
ENABLING DECISION-MAKING

- During the analysis process it was identified that access privileges within shared drives is relatively open with few restrictions. This caused ransomware events that spread to shared drives to impact a much greater volume of data on shared drives

- We ran an iteration of the current state analysis to show how aggregate risk would be reduced if access privileges were improved relative to shared drives only

ENABLING DECISION-MAKING

If access privileges were improved relative to shared drives only,
the average loss exposure would be reduced by approximately $413K



	Analysis	Reporting Period	Minimum	10th %	Average	90th %	Maximum
■	Ransomware Current State	Q2 2016	$62K	$202K	$678K	$1.4M	$4.1M
■	Ransomware w/Restricted Shared Drive Access	Q2 2016	$36K	$99K	$265K	$396K	$3.5M

KEY RANSOMEWARE CONTROLS

BACKUPS

- Key to restoring files affected by Malware
- Include full and incremental
- Tested to ensure recovery

A/V, MALWARE DETECTION

- Can prevent known signatures from affecting workstations

USER TRAINING

- Phishing is a common method used by attacker to get ransomware installed
- Anti-phishing training has not proven to be highly effective

DATA SOURCES

- Incident Response
  - Historical incidents
  - A/V logs, detection rates
- IT Operations
  - Workstation re-imaging data
  - Data on backups / testing / restoration windows
- Business Operations
  - Impact to business processes and teams
- Industry Research
  - Success rate of phishing training

DECISION SUPPORT

- Q1 of 2016 showed a rapid growth in Ransomware attacks
- We often refer to these risk scenarios as “emerging risk issues”
- FAIR-based analyses are an ideal way to help assess these new emerging risks
- By leveraging data within your organization you can rapidly quantify the exposure and communicate with internal stakeholders how significant a given issue is specific to your organization