2020

Reducing Cyber Risk from Employees Working at Home

Presented by: Christina Dulovich| RiskLens Consultant | 04.02.2020

RiskLens®

WEBINAR AGENDA

Answering the Question

Analysis Results & Review

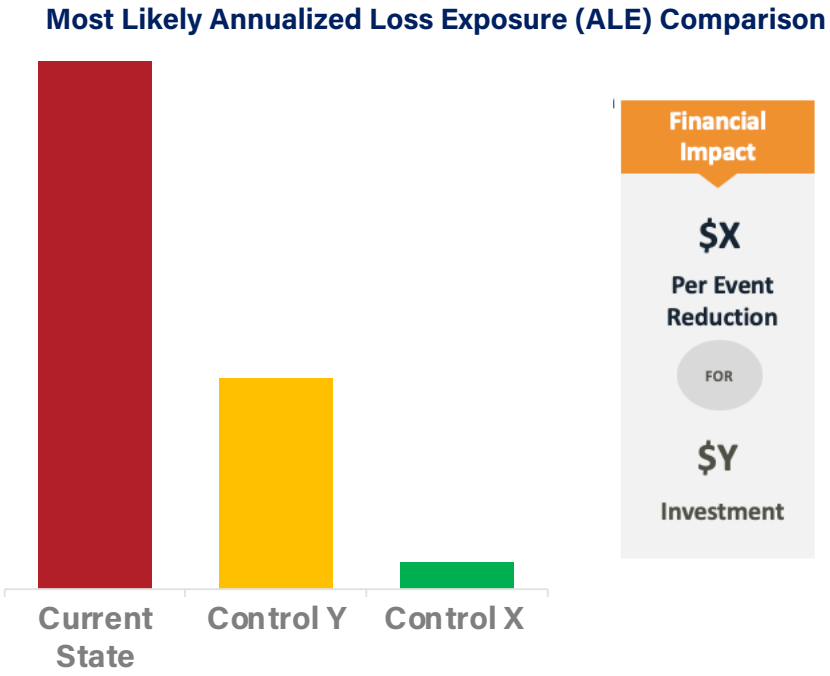
Key Takeaways

ANSWERING THE QUESTION

Given our current climate, how can we reduce our Cyber Risk related to employees working from home?

Cost- Benefit Analysis

1. Identification and analyze baseline loss event(s)
2. Determine which factor(s) of the FAIR Model are impacted
3. Update baseline analysis for FAIR Model factor(s) impacted
4. Compare analysis deltas to annualized investment cost

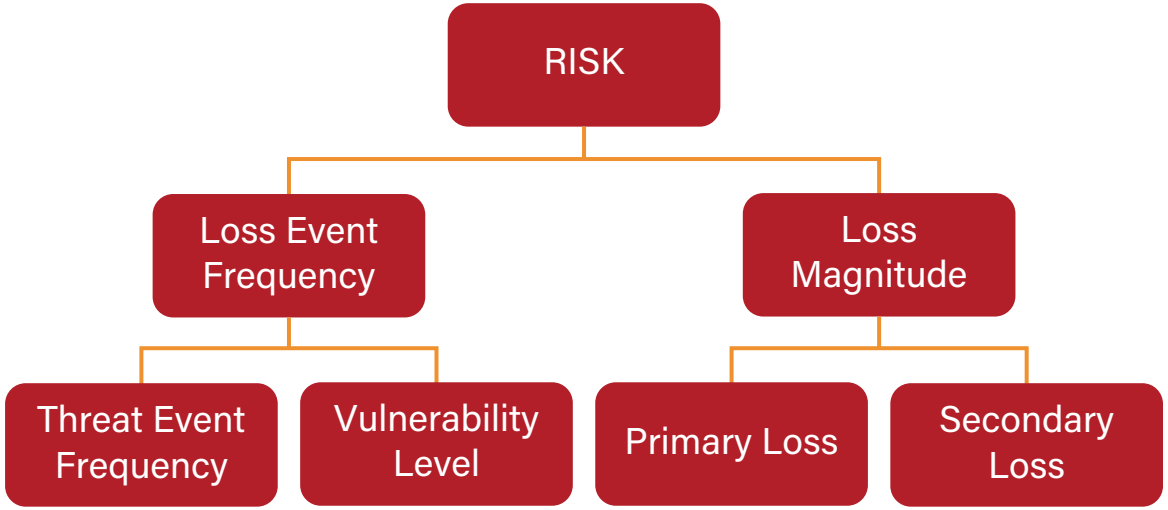


RiskLens®

HOW TO MEASURE RISK

FAIR

Factor Analysis of Information Risk



Risk = probable frequency and probable magnitude of future loss (expressed in dollars)

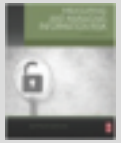
Accredited as an Industry Standard by

Complementary to Risk Frameworks

Supported by a Fast Growing Community

Wide Industry Adoption 30% Fortune 1000

FAIR Book Inducted in Cybersecurity Canon



ANALYSIS BACKGROUND

Large technology organization interested in the ability to...

FAIR Model
Rigorous Approach

RiskLens Platform

Make effective, risk-based decisions related to **protecting customer PII while employees are working from home**

RiskLens®

STEP 1: IDENTIFY BASELINE LOSS EVENT(S)

Current State = Determine how much risk is associated with an **employee** disclosing **customer PII residing on employee workstations** *via exfiltration to personal cloud solutions,* resulting in a **loss of confidentiality**

Loss Event

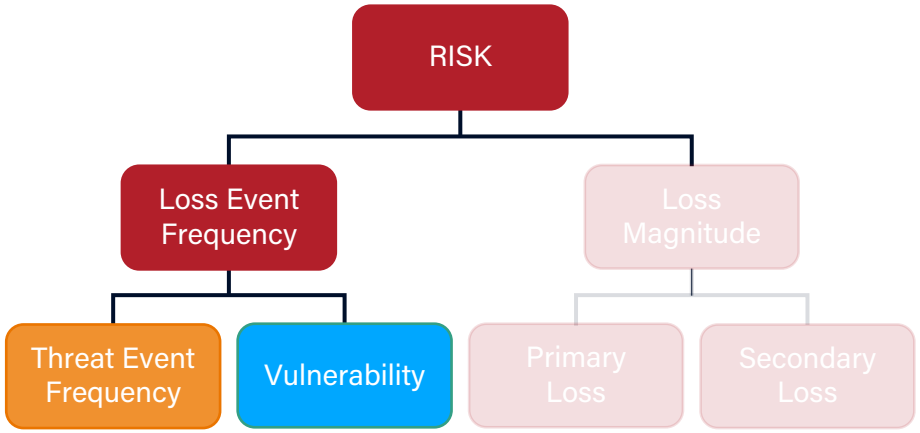
Future State: The risk reduction opportunity, in financial terms, of implementing DLP (data leak prevention) and/or blocking Cloud Hosting (IP blacklisting).

RiskLens®

STEP 1: IDENTIFY BASELINE LOSS EVENT(S)

Frequency Rationale

Factor	Definition
Threat Event Frequency	Over the next year, the # of times a privileged insider will attempt to exfiltrate customer PII residing on their workstation via uploading to unauthorized cloud storage
Vulnerability	The % of attempts by privileged insiders to exfiltrate customer PII residing on their workstation that are successful

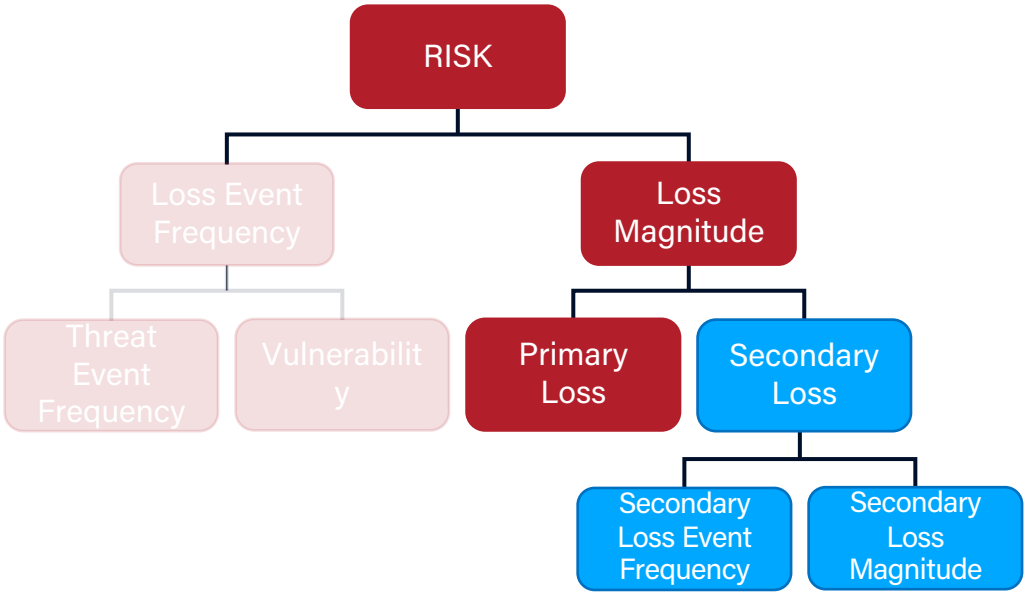


RiskLens®

STEP 1: IDENTIFY BASELINE LOSS EVENT(S)

Magnitude Rationale

Loss Magnitude represents the estimated amount of loss that could materialize **each time the loss event occurs**



Primary Loss

- Cost to investigate the event
- Cost to respond to the event

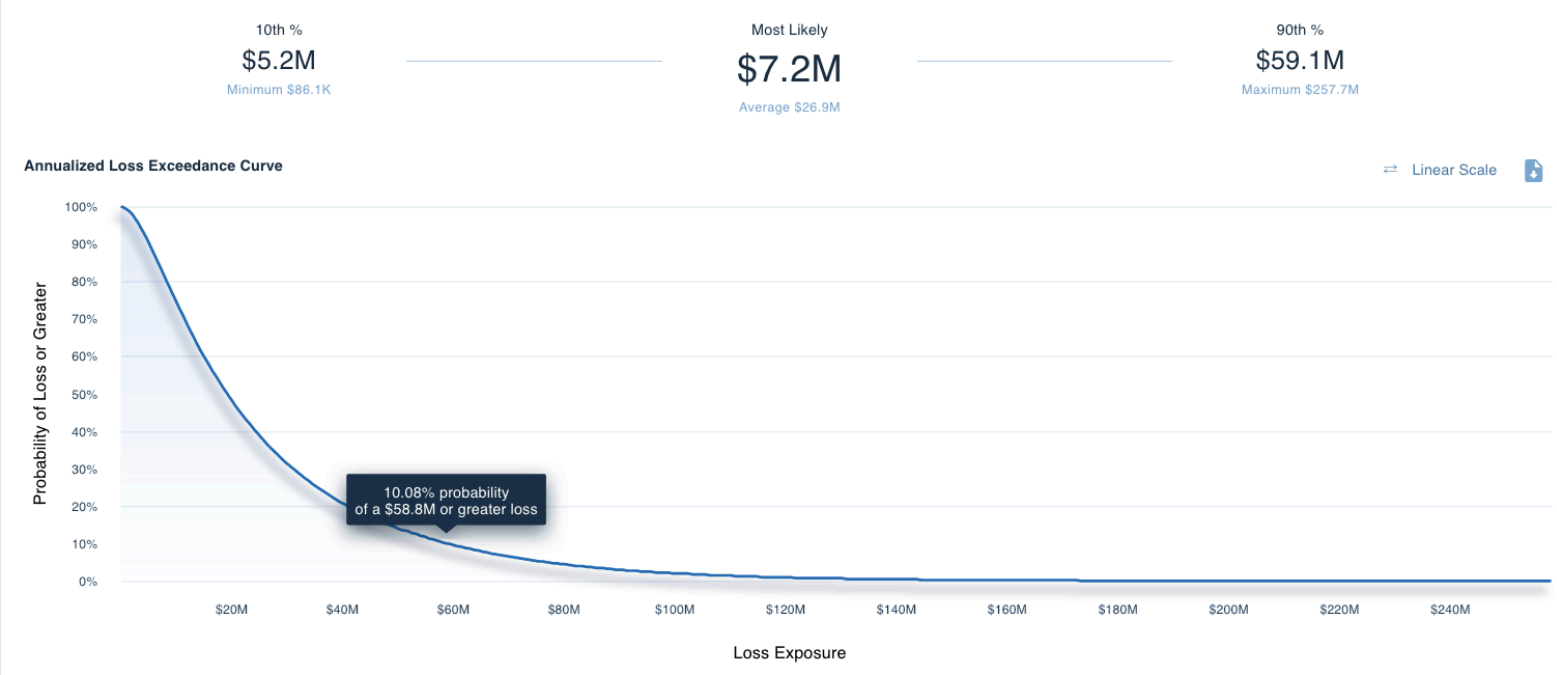
Secondary Loss

- Regulator & customer notification
- Credit Monitoring
- Litigation
- Third Party Audits
- Fines & Judgments
- Reputation Damage (customer churn)

RiskLens

STEP 1: IDENTIFY BASELINE LOSS EVENT(S)

Annualized Loss Exposure



Per event metrics

#

Min: 12 times in 1 year
Most Likely: 24 times in 1 year
Max: 365 times in 1 year

$

Primary Loss (Direct Impact): $500 - $2K
Secondary Loss (Indirect Impact) : $2.5K - $1.6M

RiskLens

STEP 2: DETERMINE IMPACTED MODEL FACTOR(S)

Isolate the factor impacted by control change

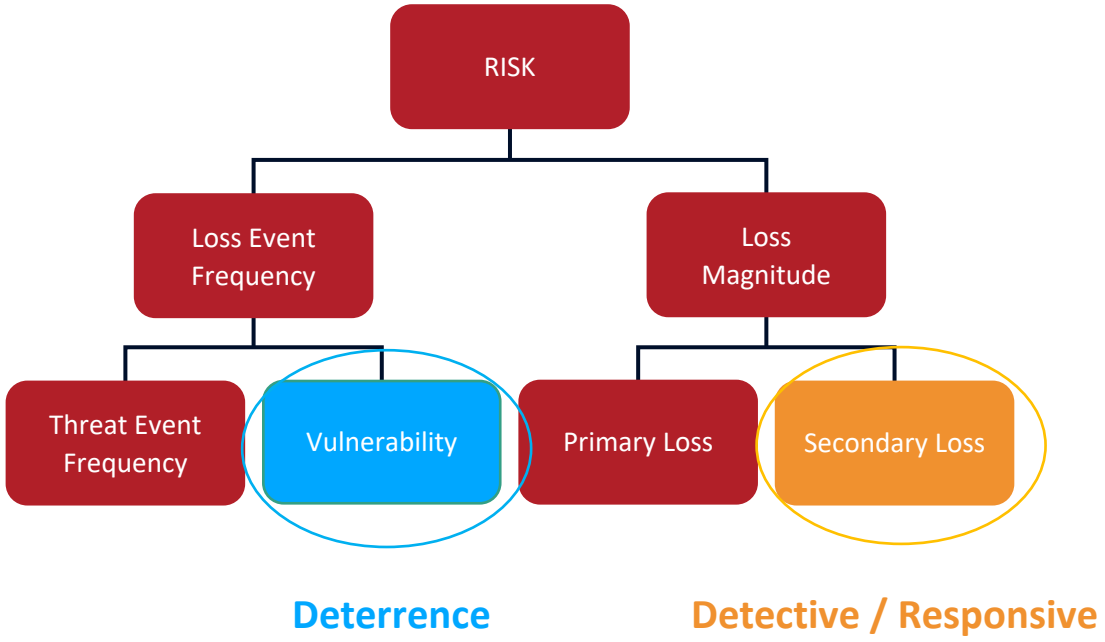
DLP *(threshold block)*

Cloud Hosting Block *(blacklisted IP addresses)*

Consider the extent of the impact

Reduction of exfiltrated records

Additional workarounds employees may take if cloud hosting sites are blocked on their workstation



RiskLens®

STEP 3: UPDATE BASELINE FAIR MODEL FACTOR(S)

Data Loss Prevention
(block above threshold)

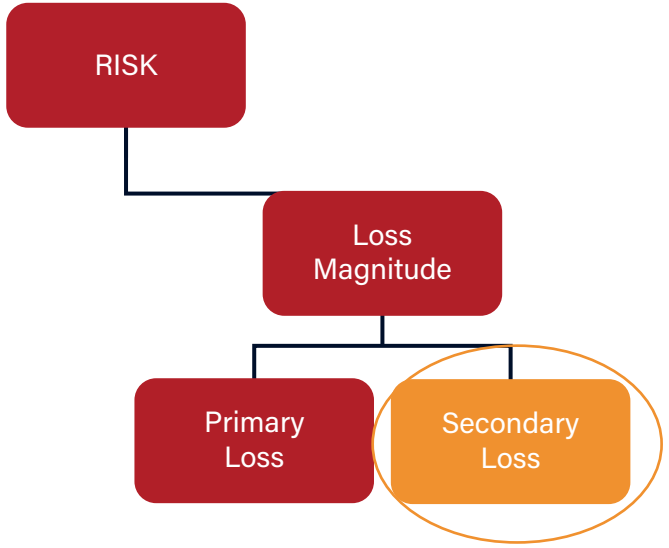
Sensitive Records

How many sensitive records (if any) are stored on or processed by these assets?

Minimum	Maximum		Most Likely
1	500	Confidence Medium	499

☑ Override

Reduction of approximately 9,500 records, that the employee has legitimate access to, being exfiltrated.



Detective / Responsive

RiskLens

STEP 3: UPDATE BASELINE FACTOR(S)

Cloud Hosting Block
(IP address blacklisting)

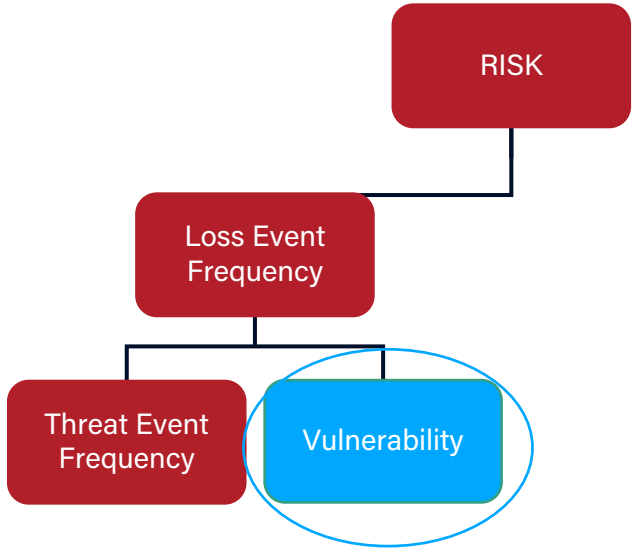
Vulnerability

What percentage of threat events are likely to result in loss events? In the rationale field, describe the source(s) and/or basis for these data.

Minimum	Maximum		Most Likely
50%	75%	Confidence Medium	62.5%

☐ Override

Reduction of likelihood that the employee would successfully exfiltrate the sensitive information to their personal cloud systems with Cloud Hosting IP addresses blacklisted.



Deterrence

RiskLens

STEP 4: COMPARE DELTAS TO INVESTMENT COST

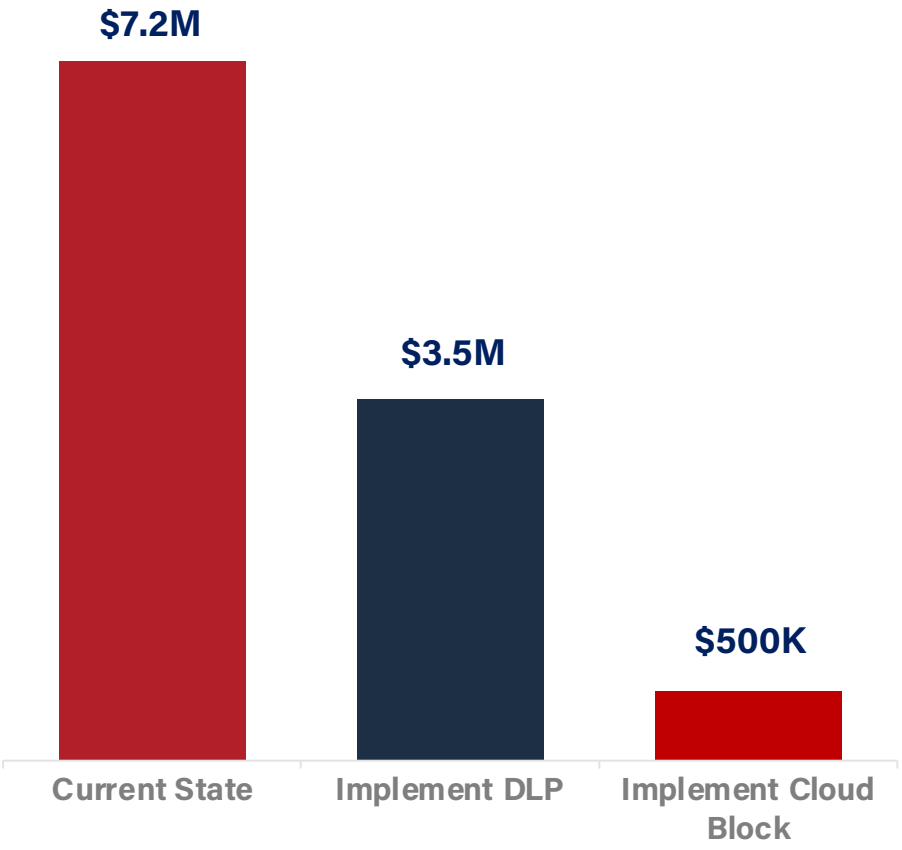
Key Driver – DLP (over a given threshold)

Reduction of potential records breached, therefore reducing the magnitude of the loss event

Key Driver – Cloud Hosting Block

Reduction in the likelihood of the exfiltration of any sensitive information to personal cloud systems

Most Likely Annualized Loss Exposure (ALE) Comparison



Cloud Block Financial Impact

$6.7M

Per Event Reduction

vs.

$X

Investment

RiskLens®

ANSWERING THE QUESTION

Which control should we invest in - to maintain control over sensitive corporate information while our employees are working from home?

Without FAIR and RiskLens:

"We need this new software/control because we're currently at **high risk** of experiencing a data breach.

The likelihood is **medium** and the impact is **high**, meaning it's a **high risk**."

With FAIR and RiskLens:

"Our Cost Benefit analysis shows that the ROI of control A exceeds the ROI of control B by $X. Here is my quantitative risk analysis to show that"

RiskLens

KEY TAKEWAYS

Cyber Risk Quantification provides the business lens you need to:

- Communication of Cyber Risk in financial terms
- Effectively prioritize remediation efforts via risk-based decisions
- Justify budget requests and demonstrate Cost Benefit Analyses

RiskLens®