CASE STUDY

Manufacturer Makes Risk-based Decision on Ransomware Controls

RiskLens

Challenges
A multinational food manufacturing company was faced with a decision of how to protect its distribution process from being impacted by a zero-day ransomware attack. Should the organization invest in additional controls to improve response time for plant outages, or should network micro-segmentation be implemented to decrease the probability of ransomware propagating across the network?

Solution
Using RiskLens, analysts determined the current exposure to a zero-day ransomware attack deployed on an employee workstation that propagates to the main system supporting operations for a key distribution facility in North America. Additionally, using RiskLens' versioning capability, the organization was able to determine the amount of risk reduction, in dollars and cents, if either additional tools/technologies are implemented to improve incident response time or if network micro-segmentation was implemented across the network.

Results
Executive management was empowered with data to make a control investment decision that produced a compelling business case that not only helped to improve executive decision-making, but also that aligned with the interests of the Board.

The Challenge

A multinational food manufacturing company was seeking to make an effective, risk-based decision on how to protect its distribution process from being impacted by a zero-day ransomware attack. Specifically, should the organization invest in additional controls to improve response time for outages or implement micro-segmentation to decrease the probability of ransomware propagating across the network? The organization's conventional approach to risk rankings could not support executive management's decision. In order to answer these questions, the organization needed to start communicating risk using a method consumable by business stakeholders (i.e., dollars and cents).

The Solution

The RiskLens platform combines an intuitive workflow process for scoping and data collection with a sophisticated analytics engine based on Factor Analysis of Information Risk (FAIR), an industry standard for the quantification of information security risk.

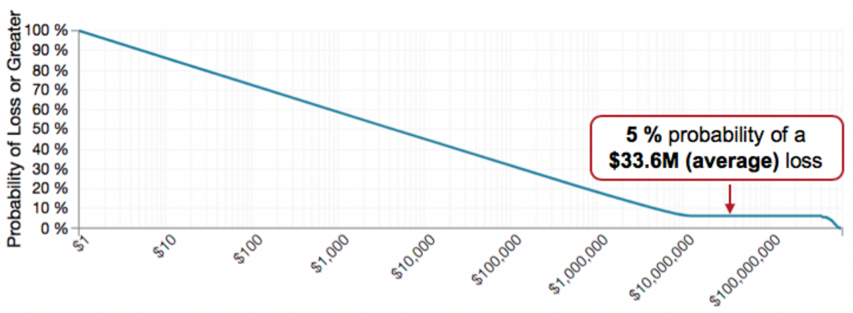
We began by focusing our analysis on the amount of risk associated with a cybercriminal deploying ransomware on an employee workstation that propagates to the main system supporting operations for a key distribution facility in North America. The scenario analyzed assumed the outage could range from 72 hours to 30 days (with partial operations resuming past 15 days). The analysts used the simple scoping capability within RiskLens to determine which data points were necessary for the analysis; effectively reducing their work load by removing research into data that did not ultimately support quantifying risk. The analysis collected data through structured workshop questions on key data points including the number of reported ransomware campaigns, the percentage of ransomware activity that successfully made it onto an employee workstation, and the percentage of campaigns involving a worm. The analysis also gathered data on the associated cost of the event if it were to materialize. Data points gathered here included the revenue lost from the inability to manufacture and distribute the product, man hours involved in incident response procedures and forensics, SLA fines imposed by customers and carriers, and relevant data points captured from the business impact assessment (BIA), including recovery time objectives (RTOs). Each data point input into the analysis was entered using distributions to account for uncertainty. One piece of information that was excluded from the analysis was reputation damage, which was elected to be excluded by management. These costs were captured in a loss table that was then stored in RiskLens to reuse on additional analysis work involving outages. Over the course of a three-day period, the organization was able to efficiently produce both high level reporting and detailed results described in financial terms.

Figure 1.1: Per Event Current State Results

.04 Frequency
Estimated loss events per year
(1 in a 25 year event)

$ **Primary Loss**: $233M - $660M
Secondary Loss: $372K - $998K

Figure 1.2: Loss Exceedance Curve



5 % probability of a **$33.6M (average)** loss

Figure 1.1 illustrates the per event metrics for the current state analysis. Based on the results of the analysis, the organization was looking at a one-in-25-year event that could yield a loss ranging from $250M to $660M. Figure 1.2 is another report that displays the results using a loss exceedance curve - illustrating the relative probability within a simulated year of a loss of a given magnitude. For example, there is a 5% probability of the organization facing a loss of $33.6M (the average loss exposure in a simulated year). Note: we called out the average value as an example since it ties to the current state value in Figure 2 below.

Key Benefits

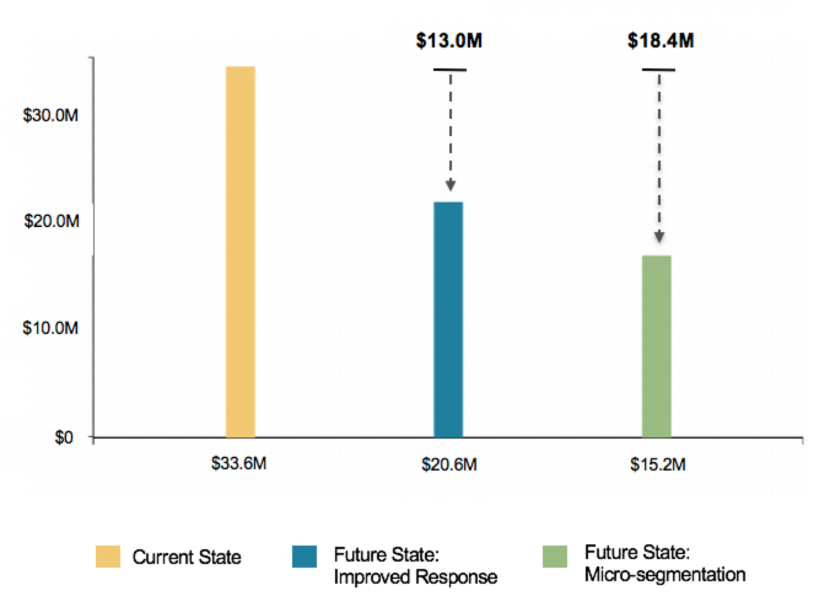
The RiskLens platform allowed the organization to rapidly quantify the loss exposure of a zero-day ransomware attack that would result in the inability to distribute product. Additionally, the level of rigor that went into the data gathering sessions led to insightful conversations amongst various areas of the business that wouldn't have otherwise been uncovered. For example, the distribution team realized they should shift their focus from disaster recovery efforts to better defining and testing recovery procedures resulting from a ransomware worm. Additionally, the data gathered for the magnitude of the loss event provided insight into future decision making for planned network downtime for maintenance purposes.

Risk Reduction Opportunities

- *Invest in additional tools / technologies to improve incident response time*
- *Implement network micro-segmentation throughout the organization*

The analyst also leveraged RiskLen's versioning capability to model several risk reduction opportunities. Figure 2 compares the loss exposure for the current state environment compared to the loss exposure once either of the two investment solutions were implemented. Combined current state loss exposure (average) was $33.6M annualized. Implementing improved incident response time decreased the loss exposure by an average of $13M on an annualized basis, and micro-segmentation led to an even larger reduction of 18.4M. The next step for management was to determine the investment cost for each of these two options. Although exact figures are not provided here, based on high-level conversations, the improved response time controls would require significantly less time and resources to implement than it would for micro-segmentation. Therefore, the additional reduction from micro-segmentation may not fully justify the cost of the investment. This analysis produced a compelling business case that not only helped to improve executive decision-making, but aligned with the interests of the Board.

Figure 2: Risk Reduction Opportunities


$13.0M
$18.4M
$30.0M
$20.0M
$10.0M
$0
$33.6M
$20.6M
$15.2M
Current State
Future State: Improved Response
Future State: Micro-segmentation