Model Details

The goal of our webpage is to provide a tool for small and medium sized businesses (SMBs) to input company characteristics and receive a cost-benefit analysis of using Rocus' Cyberfusion software. This document presents the basics of our model. We start by outlining the framework of the model. Then we discuss the details of the model's four main components: (1) cybersecurity spending, (2) probability of attack on a SMB, (3) probability of a successful attack on a SMB, and (4) the cost of an attack on a SMB.

Framework of the Model

The model calculates the estimated costs of an attack for the company with and without the use of Rocus' software . We then calculate the difference between these two costs to determine the benefit of using the Cyberfusion platform. More formally,

1. Estimated Cybersecurity Costs without Rocus =
   - (Current Cybersecurity Spending) + [P(Attack) * P(Successful Attack) * (Cost of Attack)]
2. Estimated Cybersecurity Costs with Rocus =
   - (Cost of Rocus Platform) + [P(Attack) * P(Successful Attack) * (Cost of Attack)]
3. Cost-Benefit =
   - (Estimated Cybersecurity Costs without Rocus) - (Estimated Cybersecurity Costs with Rocus)

Components of the Model

1. **Cybersecurity Spending**: The company will input into the webpage their current cybersecurity spending, which will go into the estimated cost of an attack without Rocus. Then, the company will input the number of users they wish to have on the Cyberfusion platform. The cost-benefit analysis uses this number to calculate the estimated cybersecurity spending on Rocus's platform by multiplying the number of users by $50 per month (or $600/year).
   - Input by potential client company
     - Current spending on cybersecurity
     - Number of users

2. **Probability of Attack**: In this section, we discuss how we estimate the probability of attack for a potential client company. First, we build a model predicting the probability, using data and characteristics from current Rocus clients. Second, on the Rocus webpage, we ask the potential client company to input its own values for these characteristics. Finally, we combine the initial probability and the data from the potential client to estimate the probability of attack for that client.
   - **Building a model predicting the probability of attack.** Our first step was to calculate the actual probability of attack for current Rocus clients. We received threat data over a 30-day period for 7 clients. These data included 3 types of threats (listed below). We calculated and combined probabilities as follows:

  - Endpoint Threat Probability
    - An endpoint is a company device outside the corporate firewall that connects to the central network. An endpoint threat is a threat that occurred on one of these devices.
    - (Endpoint Threat Count) / (Total Endpoint Activity)
  - Firewall Threat Probability
    - A firewall is a part of the network that is designed to block unauthorized access while permitting outward communication. A firewall threat is a threat detected by the firewall and can be classified as informational, low, medium, high, or critical depending on the content.
    - (Critical Threat Count + High Threat Count) / (Total Firewall Threat Count)
  - Proxy Threat Probability
    - A proxy threat is an inside out threat where someone tries to break into the encrypted network.
    - (Total Count Proxy Threats) / (Total Count Proxy Activity/All)
  - From these three probabilities, we calculated a single probability of attack for each client company:
    - P(Attack) = P(Endpoint Threat) OR P(Firewall) OR (Proxy Threat)
    - $P(A \cup B \cup C) = P(A) + P(B) + P(C) - P(A \cap B) - P(A \cap C) - P(B \cap C) + P(A \cap B \cap C)$
- Our second step in building the model was to collect additional data about the 7 client companies, specifically characteristics that might relate to the probability of attack. The additional data covered covered 33 characteristics (see the Codebook for full descriptions). We then estimated a range of bivariate regression models, comparing each characteristic (the independent variable) to the probability of attack (the dependent variable). Our goal was to select a small number of company characteristics that were closely related to the probability of attack. Across the 33 bivariate models, 4 characteristics produced an R-squared value of greater than .45: number of employees, estimated revenue, current cybersecurity spending, and number of endpoints.
- For our final step in building the model, we estimated a multivariate model in which the dependent variable was the probability of attack, and the independent variables were the 4 company characteristics mentioned immediately above. The adjusted R-squared value for this model was .83, indicating that the model explains 83% of the variation in the probability of attack (the dependent variable). These multivariate results became our model predicting the probability of attack.
- **Requesting data from the potential client company.** The Rocus web page asks a potential client company to input the four characteristics (number of employees, estimated revenue, current cybersecurity spending, and number of endpoints).
- **Estimating the probability of attack for the client company.** The webpage then combines the inputted values and the coefficients from the multivariate model, and the result is the estimated probability of attack for the client company.

3. **Probability of Successful Attack:** The probability of a threat being a successful attack is dependent on a company’s cybersecurity software. According to Kaspersky Lab’s 2016 Report: Measuring the Financial Impact of IT Security on Businesses, 43% of all incidents experienced by businesses resulted in a data breach, loss, or exposure. Therefore, without Rocus’s platform, we estimate the probability of a successful attack with a baseline of $7500 in cybersecurity spending as 43%. We estimate a gain of 0.5% success rate with the additional spending of $1500 until reaching $15000, symmetric to the loss rate until $0 spending. Using Rocus’s platform, the probability of a successful attack is only 0.1%. This latter number is based on the experience of current Rocus clients.
    - Probability calculation based on current cybersecurity spending

$1500 or less	41%
$3000	41.5%
$4500	42%
$6000	42.5%
$7500	43%
$9000	43.5%
$10500	44%
$12000	44.5%
$13500	45%
$15000 or more	45.5%

    - Input by potential client company
        - Current cybersecurity spending

4. **Cost of Attack:** The cost of a data breach is a key factor in determining the cost of an attack overall. The company inputs their estimated percentage of clients lost to a data breach and their estimated revenue per year. These two values are then multiplied to determine the overall cost of the attack.
    - Input by potential client company
        - Estimated revenue per year
        - Estimated percentage of clients lost to a data breach