Data Explanation

Variables

- Each row represents a different company for the variables in the columns

Num Employees

- Number of employees at the company

Estimated Revenue

- Estimated revenue per fiscal year in dollars

Company City Population

- Population of the city of which the company is headquartered

Company Region

- Region in which the company is headquartered
    - Southeast region
        - Delaware, West Virginia, Virginia, Maryland, Tennessee, Kentucky, Arkansas, Alabama, Mississippi, Louisiana, Georgia, Florida, South Carolina, North Carolina
            - 1: yes
            - 0: no
    - Northeast region
        - Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, Connecticut, New York, New Jersey, Pennsylvania
            - 1: yes
            - 0: no
    - Southwest region
        - Arizona, New Mexico, Texas, Oklahoma
            - 1: yes
            - 0: no
    - West region
        - Washington, Oregon, California, Nevada, Utah, Colorado, Wyoming, Montana, Idaho
            - 1: yes
            - 0: no
    - Midwest region
        - Ohio, Illinois, Indiana, Michigan, Minnesota, Wisconsin, Missouri, Iowa, Kansas, Nebraska, North Dakota, South Dakota
            - 1: yes
            - 0: no

PPI?

- Protected Personal Information

- 1: yes
- 0: no

PII?
- Personal Identifiable Information
- 1: yes
- 0: no

PCI?
- Payment Card Industry
- 1: yes
- 0: no

Type of Data
- Client data
    - 1: yes
    - 0: no
- Intellectual property and trade secrets
    - 1: yes
    - 0: no

Industry: Which industry is the company in?
- Financial Services
    - 1: yes
    - 0: no
- Professional Services
    - 1: yes
    - 0: no
- Manufacturing
    - 1: yes
    - 0: no
- Government/Public sector
    - 1: yes
    - 0: no
- Aerospace & Defense
    - 1: yes
    - 0: no
- Education
    - 1: yes
    - 0: no
- Transportation
    - 1: yes
    - 0: no

- Health
    - 1: yes
    - 0: no
- Food & Hospitality
    - 1: yes
    - 0: no
- Real Estate
    - 1: yes
    - 0: no
- Energy
    - 1: yes
    - 0: no

Firewall?

- Does the company have an existing firewall?
- 1: yes
- 0: no

AV?

- Does the company use an anti-virus software?
- 1: yes
- 0: no

Security Monitoring?

- Does the company use security monitoring?
- 1: yes
- 0: no

Percentage of clients lost to data breach

- Percentage 0 to 1

Current Cybersecurity Spending (on Rocus)

- Cybersecurity spending on Rocus software per year

AV (Type)

- Does the company use Rocus's anti-virus software?
- 1: yes
- 0: no

Firewall (Type)

- Does the company use Rocus's firewall?
- 1: yes
- 0: no

Proxy Server (Type)

- Does the company use Rocus's proxy server?
- 1: yes
- 0: no

Number of Endpoints

- Number of company devices outside the corporate firewall that connect to the central network

End Point Threat Count

- Number of threats that occured on devices outside the corporate firewall that connect to the central network

End Point Threat Probability

- Percentage 0 to 1
    - (Endpoint Threat Count) / (Total Endpoint Activity) over a 30 day period

End Point ScriptControls

- Number of ScriptControls or the number of events that were not bad on the Endpoints

End Point Exploit Attempts

- Number of Exploit Attempts or the number of events that had around a 50 percent chance of being bad on the Endpoints

Informational Firewall Data Num

- Count of informational data (alerts that are purely reported for information) for the company's' firewall (a software program or piece of hardware that helps screen out hackers and viruses)

Low Firewall Data Num

- Count of low data (issues that do not have any significant impact and are not exploitable) for the company's firewall (a software program or piece of hardware that helps screen out hackers and viruses))

Medium Firewall Data Num

- Count of medium data (small impact vulnerabilities that are still addressed) for the company's firewall (a software program or piece of hardware that helps screen out hackers and viruses)

High Firewall Data Num

- Count of high data (vulnerabilities that could lead to hacking or eventually an even larger impact) for the company's firewall (a software program or piece of hardware that helps screen out hackers and viruses)

Critical Firewall Data Num

- Count of critical data (vulnerabilities that give attackers full access) for the company's firewall (a software program or piece of hardware that helps screen out hackers and viruses)

Firewall Probability

- Percentage 0 to 1
    - (Critical Threat Count + High Threat Count) / (Total Firewall Threat Count) over a 30 day period

Blocked URL Proxy All Count

- Count of blocked URLs for all company proxy data (a function that is used to obtain inside out data by other computers)

Alert Proxy All Count

- Count of alerts for all company proxy data (a function that is used to obtain inside out data by other computers)

Blocked URL Proxy Threat Count

- Count of blocked URLs for all company proxy threats (malware that is known to act as a proxy server, allowing malicious users to utilize the affected systems in order to hide their identities by blocking their URL)

Alert Proxy Threat Count

- Count of alerts for all company proxy threats (malware that is known to act as a proxy server, allowing malicious users to utilize the affected systems with alerts)

Unknown Proxy Threat Count

- Count of all unknown threats for all company proxy threats (malware that is known to act as a proxy server, allowing malicious users to utilize the affected systems)

Proxy Avoidance and Anonymizers Threat Count

- Count of all proxy avoidance and anonymizers threats for all company proxy threats (malware that is known to act as a proxy server, allowing malicious users to utilize the affected systems in order to hide their identities by making the activity untraceable)

Malware Proxy Threat Count

- Count of all malware threats for all company proxy threat (malware that aims to damage or disable computers and computer systems)

Phishing Proxy Threat Count

- Count of all phishing threats for all company proxy threats (sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information)

Hacking Proxy Threat Count

- Count of all hacking threats for all company proxy threats (malware that is known to act as a proxy server, allowing malicious users to utilize the affected systems)

Command and Control Proxy Threat Count

- Count of all command and control threats for all company proxy threats (malware that is used by attackers to maintain communications with compromised systems within a target network)

Proxy Threat Probability

- Percentage 0 to 1
    - (Total Count Proxy Threats) / (Total Count Proxy Activity/All) over a 30 day period