Company Risk Scoring: A Comprehensive Approach to Cybersecurity Assessment

Introduction and Overview

Organizations face an ever-evolving array of cybersecurity threats in today's interconnected digital landscape. The increasing sophistication of cyber attacks, coupled with the expanding attack surface due to cloud adoption, remote work, and complex supply chains, has made robust cybersecurity risk assessment more critical than ever. This white paper describes a comprehensive approach to company risk scoring (hereinafter – **Scoring**), outlining how organizations can gain a clear and actionable understanding of their cybersecurity posture.

Purpose and Scope

The purpose of this white paper is to detail a multi-faceted Scoring methodology that leverages diverse data sources and advanced analytics to produce a comprehensive assessment of an organization's cybersecurity risks and risk score (hereinafter – **the Score**). Our approach goes beyond traditional vulnerability assessments, incorporating a wide range of factors that contribute to an organization's overall security posture.

This document will:

1. Explain the importance of comprehensive cybersecurity risk assessment
2. Detail the methodology behind our Scoring system
3. Explore the various risk factors considered in our assessment
4. Discuss the implementation and interpretation of the Scores
5. Provide insights into risk mitigation strategies based on assessment results

Our Approach to Scoring

Our Scoring methodology provides a framework for evaluating an organization's cybersecurity posture, incorporating data from multiple sources and considering various aspects of security. Key features of our approach include:

- **Multi-factor Assessment**: We consider risks across seven key domains, including software patching, web application security, email security, system reputation, SSL configuration, system hosting, and data breach history.

- **Data-driven Analysis**: Our system compiles data from reputable sources such as IOT search engines, IP and/or domain reputational databases, and custom security scans to produce Scores.

- **Customizable Scoring**: While we provide the Score, our system also allows for a detailed examination of individual risk factors, enabling organizations to focus on specific areas of concern.

- **Actionable Insights**: Beyond generating scores, our system provides contextual information to support organizations in identifying and addressing potential vulnerabilities and/or weak spots.

- **Scalable Architecture**: Our Scoring system is designed to support evaluations for organizations of all sizes, from small businesses to large enterprises.

In the following sections, we will delve into the details of our risk scoring methodology, exploring each risk factor, our data collection and processing techniques, and how we translate raw data into meaningful, actionable Scores. By the end of this white paper, readers should have a comprehensive understanding of our approach to company risk scoring and how it may be applied to enhance their organization's cybersecurity posture.

Background Research

To provide a comprehensive understanding of our Scoring methodology, it's essential to examine the existing landscape of cybersecurity risk assessment. This section will explore current practices, methodologies, and standards in the field, as well as how our approach builds upon and extends these concepts.

Our Approach in Context

Our Scoring methodology aims to address limitations of currently available solutions in the market by:

1. **Comprehensive Coverage**: Our methodology may incorporate CVSS metrics alongside additional factors from various data sources to provide a broader view of potential cybersecurity risks, enhancing the understanding of an organization's security posture.

2. **Quantitative and Qualitative Insights**: Similar to FAIR, we provide quantitative scores, but we also may offer qualitative insights and recommendations, which could make our assessments more actionable.

3. **Alignment with Best Practices**: Our methodology may incorporate elements from established frameworks and/or standards like NIST and ISO 27001, aiming to align with industry best practices.

4. **External Factors**: Our methodology leverages external data sources, such as security rating services, to assess an organization's cybersecurity posture based on publicly available information. When combined with insights from an organization's internal security assessments, this approach should provide a more comprehensive understanding of potential vulnerabilities and/or weak spots.

5. **Automated and Scalable**: Our system autonomously conducts scalable assessments through a fully automated codebase, performing scoring and evaluations without the need for human intervention, thereby eliminating the potential for human error.

Key Components of Our Implementation

Our Scoring methodology incorporates several key components:

1. **Multi-factor Assessment**: We evaluate risks across seven key risk factors:

    - Software Patching
    - Web Application Security
    - Email Security
    - System Reputation
    - SSL Configuration
    - System Hosting

- Data Breach History

2. **Data Integration**: Our system integrates data from multiple sources, including:

    - IOT Search engines for internet-facing asset discovery and vulnerability assessment
    - IP and/or Domain name reputation databases for tracking and identifying malicious IP addresses
    - Custom scanners for email security, SSL configuration, and web application vulnerabilities

3. **Scoring Algorithms**: We use sophisticated algorithms to calculate both individual factor scores and an overall Score. These algorithms take into account the severity and prevalence of detected issues, as well as the relative importance of different risk factors.

4. **Normalization and Contextualization**: Our Scoring system normalizes results based on various factors, allowing for meaningful comparisons between different entities.

5. **Continuous Monitoring**: The system is designed for ongoing assessments, allowing organizations to track their security posture over time and quickly identify new weak points or emerging threats.

By combining these elements, our approach aims to provide a more comprehensive, nuanced, and actionable view of cybersecurity risk than many existing methodologies. In the following sections, we will delve deeper into each component of our Scoring system, explaining how we collect and analyze data, calculate Scores, and generate actionable insights.

Methodology Overview

Our Scoring methodology is designed to provide a comprehensive, easy-to-understand assessment of an organization's cybersecurity posture. By examining multiple aspects of security and using advanced analysis techniques, we aim to deliver insights that can guide security efforts and resource allocation. This section provides an overview of our approach, explaining the key components and processes involved in generating the Score.

Core Principles

Our methodology is built on several core principles:

1. **Comprehensive Coverage**: We look at multiple aspects of an organization's cybersecurity, providing a well-rounded view of potential vulnerabilities and risks.

2. **Data-Driven Approach**: Our assessments are based on measurable facts rather than subjective opinions.

3. **Continuous Monitoring**: The system performs regular assessments, allowing organizations to track their security status over time.

4. **Actionable Insights**: Beyond just providing Scores, we may offer explanations and/or recommendations to guide improvement efforts.

5. **Scalability**: Our approach can be applied to organizations of all sizes and across different industries.

Key Components

Our risk scoring system consists of several key parts:

1. **Data Collection**: We gather information from multiple sources, including internet search engines, reputation databases, and custom security checks.

2. **Data Processing**: The collected information is organized and analyzed to extract relevant security insights.

3. **Scoring Engine**: This component calculates individual scores for different security aspects and combines them into the Score.

Risk Factors, Categories and Process Flow

We assess risk across seven key areas:

1. **Software Patching**: How well the organization keeps its software up-to-date.
2. **Web Application Security**: The safety of the organization's websites and web-based applications.

3. **Email Security**: Measures taken to protect email communications.
4. **System Reputation**: Whether the organization's systems have been associated with any malicious activity.
5. **SSL Configuration**: The proper use of encryption for secure communications.
6. **System Hosting**: How and where the organization's systems are set up and maintained.
7. **Data Breach History**: Past incidents of data loss or theft and their impact.

The Scoring process then follows these general steps:

1. **Gathering Data**: The system collects data about the target organization from various sources.

2. **Organizing and Analyzing Information**: The collected data is sorted and examined to identify security strengths and weaknesses.

3. **Calculating Scores**:
   a. The system assigns scores to each of the seven risk factors based on the analyzed data.
   b. These risk factors are grouped into four categories. Each category is scored on a scale of 0-100, calculated by summing the scores of the relevant risk factors, dividing by the number of risk factors in that category, and multiplying the calculated value by 10.

4. **Overall Assessment**: The seven factor scores are combined, with some factors given more importance than others, to create the Score.

Risk factors are grouped into categories as follows:

- **Phishing and Malware**
  - Data Breach History
- **Network Security**
  - Software Patching
  - System Hosting
  - System Reputation
- **Email Security**
  - Email Security
- **Website Security**
  - Web Application Security
  - SSL Configuration

This structured grouping allows for a more nuanced assessment of each category.

The final Scores are graded as follows:

Score A (low risk)	Overall calculated value from 95 to 100

Score B (medium risk)	Overall calculated value from 90 to 94
Score C (moderate risk)	Overall calculated value from 80 to 89
Score D (high risk)	Overall calculated value from 70 to 79
Score F (critical risk)	Overall calculated value from 0 to 70

Scoring Methodology

Our scoring system assesses individual risk factors on a scale from 0 to 10, where a score of 10 suggests the lowest possible risk and optimal security, while a score of 0 indicates a higher potential risk. The Score, along with each category score, is intended to provide a comprehensive evaluation on a scale from 0 to 100.

Detailing the Calculation:

- **Individual Risk Factors:** Each of the seven risk factors is evaluated with scores ranging from 0 (indicating higher potential risk) to 10 (indicating lowest potential risk). These scores are then weighted based on their significance to the organization's overall security.
- **Grouping and Category Scores:** Risk factors are grouped into categories. The score for each category is calculated by summing the scores of the risk factors within that category, dividing by the number of factors in the category, and then normalizing to a score out of 100.
- **Overall Security Score:** The final security score is derived by aggregating the normalized category scores, adjusted according to predefined weightings.

This methodology is designed to give an indicative overview of the organization's security posture by evaluating and quantifying risk at both granular and aggregated levels, facilitating strategic decision-making and risk management.

The following table shows how much each factor contributes to the final Score:

Risk Factor	Weight
Software Patching	30%
Web Application Security	15%
Email Security	15%
System Reputation	5%
TLS/SSL Configuration	5%

Risk Factor	Weight
System Hosting	5%
Data Breach History	25%

Software Patching and Data Breach History are given the highest weights, reflecting their critical importance to an organization's overall security posture. Web Application Security and Email Security are also significant contributors. The remaining factors, while still important, have a smaller impact on the overall Score.

This weighting system aims to accurately reflect the most important aspects of an organization's security posture. For example, an organization might have excellent System Hosting practices, but if their Software Patching is poor, it will have a much larger negative impact on their Score.

Continuous Improvement

Our methodology may change. We constantly refine our approach based on:

- New types of cyber threats
- Improvements in security technologies and practices
- Feedback from users and security experts
- Analysis of how well our Scores predict actual security incidents

By keeping our approach up-to-date, we aim to have our Scoring relevant and effective in the face of ever-changing cybersecurity challenges.

In the following sections, we will explore each component of our methodology in more detail, explaining how we collect and analyze data, calculate Scores, and provide recommendations for improving security.

Detailed Exploration of Risk Factors

Our Scoring methodology assesses seven key areas of cybersecurity. Each of these risk factors contributes to the overall security posture of an organization. In this section, we'll explore each factor in detail, explaining what it measures, why it's important, and how we assess it.

1. Software Patching (30% of overall Score)

What it measures: Software Patching assesses how well an organization keeps its software up-to-date with the latest security fixes.

Why it's important: Outdated software often contains known vulnerabilities that threat actors might exploit. Regularly applying patches is one of the most effective ways to prevent cyber attacks.

How we assess it: We scan the organization's internet-facing systems to identify the versions of software in use. We then compare these versions against databases of known vulnerabilities to determine if any systems are running outdated, vulnerable software.

Key metrics:

- Number of systems with critical vulnerabilities
- Average time to patch critical vulnerabilities
- Percentage of systems running up-to-date software

2. Web Application Security (15% of overall Score)

What it measures: This factor evaluates the security of an organization's websites and web-based applications.

Why it's important: Web applications are often the primary interface between an organization and its customers or users. Vulnerabilities in these applications can lead to data breaches, financial fraud, or service disruptions.

How we assess it: We use automated scanners to check for common web vulnerabilities and insecure configurations. We also examine the use of security headers and other best practices.

Key metrics:

- Number of detected vulnerabilities
- Severity of detected vulnerabilities
- Use of security headers and best practices

3. Email Security (15% of overall Score)

What it measures: Email Security assesses the measures an organization has in place to protect its email communications.

Why it's important: Email is a primary vector for cyber attacks, including phishing and malware distribution. Strong email security can significantly reduce an organization's risk.

How we assess it: We check for the implementation and proper configuration of email authentication measures such as SPF, DKIM, and DMARC across various (sub)domains of an organization's mail servers and/or mailboxes to evaluate anti-spoofing capabilities. We also evaluate the organization's anti-spam measures and email encryption practices.

Key metrics:

- Implementation of SPF, DKIM, and DMARC
- Strength of DMARC policy
- Use of email encryption

4. System Reputation (5% of overall Score)

What it measures: System Reputation looks at whether an organization's IP addresses or domains have been associated with malicious activity.

Why it's important: If an organization's systems are compromised and used for spam or attacks, it can damage the organization's reputation and lead to blacklisting, affecting business operations.

How we assess it: We check the organization's IP addresses and domains against various reputation databases and blacklists. We also look for signs of potential compromise, such as unexpected open ports or services.

Key metrics:

- Presence on reputation blacklists
- Historical malicious activity
- Unexpected open ports or services

5. TLS/SSL Configuration (5% of overall Score)

What it measures: TLS/SSL Configuration assesses how effectively an organization implements encryption protocols to secure communications.

- **Why it's important:** Proper SSL/TLS configuration is essential for safeguarding data in transit, ensuring that communications between clients and servers remain confidential and maintain their integrity.

How we assess it: We examine the SSL/TLS certificates used by the organization's websites and services, checking for proper configuration, use of strong protocols and ciphers, and absence of known vulnerabilities.

Key metrics:

- SSL/TLS protocol versions in use
- Strength of encryption ciphers
- Validity and proper configuration of SSL/TLS certificates

6. System Hosting (5% of overall Score)

What it measures: System Hosting assesses how and where an organization's systems are set up and maintained.

Why it's important: The way systems are hosted can affect their security, reliability, and resilience to attacks. For example, using reputable cloud providers with strong security measures can enhance an organization's security posture.

How we assess it: We analyze the hosting arrangements for the organization's systems, looking at factors such as the use of content delivery networks (CDNs), cloud hosting providers, and geographic distribution of systems.

Key metrics:

- Use of reputable hosting providers
- Implementation of CDNs
- Geographic distribution of systems

7. Data Breach History (25% of overall Score)

What it measures: This factor considers any past incidents where an organization's data was compromised or stolen.

Why it's important: Past data breaches can indicate weaknesses in an organization's security practices. They also increase risk, as exposed data can be used in future attacks.

How we assess it: We research public breach databases and news sources for any reported incidents involving the organization. We also look for signs of data associated with the organization appearing on dark web markets or forums.

Key metrics:

- Number and scale of past breaches
- Types of data exposed in breaches
- Time since last known breach

By thoroughly assessing these seven risk factors, we can build a comprehensive picture of an organization's cybersecurity posture. This multi-faceted approach allows us to identify specific areas of strength and weakness, providing actionable insights for improving overall security.

In the next section, we'll explore how we collect and process the data needed to assess these risk factors.

Scoring Algorithm

Our Scoring algorithm is designed to translate complex cybersecurity data into clear, actionable scores. This section explains how we calculate both individual factor scores and the overall Score, providing insight into the principles that guide our Scoring process.

Principles of Our Scoring Approach

1. **Normalized Scoring**: We use a consistent 0-10 scale for each assessed risk factor score, where 10 represents the best possible security (lowest risk) and 0 represents the highest risk. This makes it easy to compare different factors and understand the overall risk level.

2. **Severity-Based Scoring**: Issues are weighted based on their severity. For example, a critical vulnerability in a widely-used system would have a much larger impact on the score than a low-risk issue in a non-critical system.

3. **Size Normalization**: We adjust our Scoring based on the size of the organization to have fair comparisons between small businesses and large enterprises.

4. **Industry Benchmarking**: Scores are calculated with consideration for industry standards and best practices, allowing organizations to see how they compare to their peers.

Calculating Factor Scores

For each of the seven risk factors, we follow these general steps to calculate the Score:

1. **Data Collection**: We gather all relevant data points for the factor. For example, for Software Patching, this would include information about all detected software versions and known vulnerabilities.

2. **Issue Identification**: We identify specific issues or vulnerabilities within the collected data.

3. **Severity Assignment**: Each identified issue is assigned a severity level based on its potential impact and the context in which it was found.

4. **Score Calculation**: We start with a perfect score of 10 and subtract points based on the number and severity of issues found. The more severe the issues and the more of them there are, the lower the risk factor score will be.

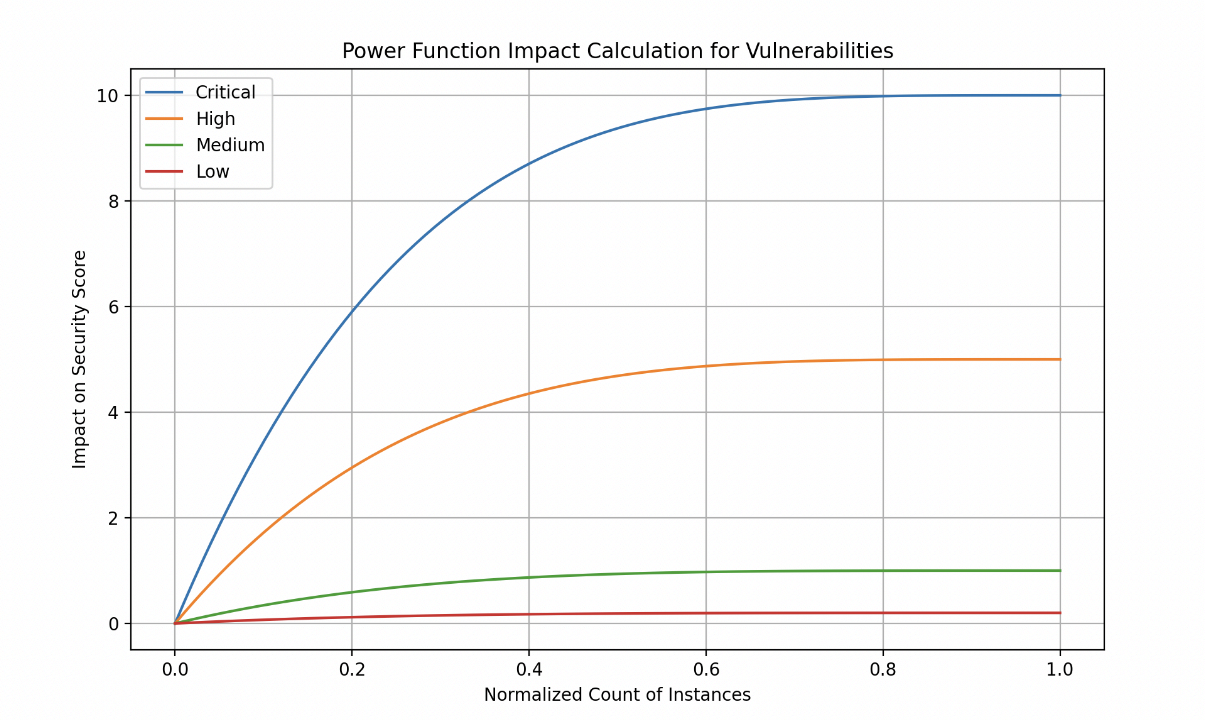
5. **Normalization**: The resulting score is normalized to ensure it fits within our 0-10 scale.

To illustrate this process, let's use an analogy of grading a test:

Imagine you're grading a 100-question test. You start with a perfect score of 100 and subtract points for each wrong answer. Some questions are worth more points than others because they're more important. At the end, you convert the score to a 0-10 scale. This is similar to how we calculate our factor scores, with cybersecurity issues taking the place of wrong answers.

Impact Calculation for Vulnerabilities

A crucial aspect of our Scoring algorithm is how we calculate the impact of vulnerabilities on the Score. To illustrate this, let's look at a chart that shows how the number of vulnerabilities affects the Score for different severity levels:



This chart illustrates several important principles of our Scoring methodology:

1. **Severity Levels**: We categorize vulnerabilities into four severity levels: Critical, High, Medium, and Low. As you can see from the chart, each severity level has a different impact on the Score.

2. **Non-Linear Impact**: The lines on the chart are curved, not straight. This shows that the impact of vulnerabilities on the Score is not linear. In other words, as the number of vulnerabilities increases, their impact on the Score grows more quickly.

3. **Different Weights for Different Severities**: Notice how the lines for different severity levels rise at different rates. The line for Critical vulnerabilities rises much more steeply than the line for Low vulnerabilities. This reflects our principle that more severe vulnerabilities have a greater impact on the Score.

4. **Diminishing Returns**: As the lines approach the right side of the chart, they start to level off. This represents the principle of diminishing returns in our scoring system. While the first few vulnerabilities of a given severity have a significant impact on the score, additional vulnerabilities of the same severity have less and less additional impact.

5. **Normalized Count**: The horizontal axis represents a "normalized count" of vulnerabilities. This means we're looking at the number of vulnerabilities relative to the size of the system or organization, not just the raw number. This helps to get fair comparisons between organizations of different sizes.

To put this into practical terms, let's consider an example:

Imagine we're assessing two different companies. Company A has a few critical vulnerabilities, while Company B has many low-severity vulnerabilities. Based on this chart, we can see that even a small number of critical vulnerabilities (represented by the blue line) could have a larger impact on the security score than a larger number of low-severity vulnerabilities (represented by the red line). This aligns with real-world security practices, where addressing critical vulnerabilities is typically prioritized over addressing a large number of low-risk issues.

This approach to calculating impact allows our scoring system to provide a nuanced view of an organization's security posture. It emphasizes the importance of addressing high-severity issues, while still accounting for the cumulative effect of lower-severity problems.

Calculating the Overall Score

To calculate the Score, we combine the seven factor scores using a weighted average. As we discussed in the Methodology Overview, each factor is assigned a specific weight based on its importance to overall security:

- Software Patching: 30%
- Web Application Security: 15%
- Email Security: 15%
- System Reputation: 5%
- SSL Configuration: 5%
- System Hosting: 5%
- Data Breach History: 25%

The weighted average is calculated by multiplying each factor score by its weight, summing these values, and then dividing by the sum of the weights (which is 100% or 1).

Here's a simplified example:

Let's say a company has the following factor scores:

- Software Patching: 8

- Web Application Security: 7
- Email Security: 9
- System Reputation: 10
- SSL Configuration: 6
- System Hosting: 8
- Data Breach History: 5

To calculate the overall score:

1. Multiply each score by its weight:

    - Software Patching: 8 x 0.30 = 2.40
    - Web Application Security: 7 x 0.15 = 1.05
    - Email Security: 9 x 0.15 = 1.35
    - System Reputation: 10 x 0.05 = 0.50
    - SSL Configuration: 6 x 0.05 = 0.30
    - System Hosting: 8 x 0.05 = 0.40
    - Data Breach History: 5 x 0.25 = 1.25

2. Sum these values: 2.40 + 1.05 + 1.35 + 0.50 + 0.30 + 0.40 + 1.25 = 7.25

3. Multiply the summed value by ten to get the final Score

The final Score for this company would be 72.5 out of 100.

Continuous Refinement

Our Scoring algorithm is not static. We continuously refine it based on:

- New threat intelligence
- Feedback from security experts and users
- Analysis of how well our Scores predict actual security incidents

This ensures that the Scores remain relevant and actionable in the face of evolving cybersecurity challenges.

Limitations and Considerations

While our Scoring methodology provides valuable insights into an organization's cybersecurity posture, it's important to understand its limitations and consider several key factors when interpreting and acting on the results. This section outlines some of the constraints of our approach and important considerations for users of our Scoring system.

Limitations of Our Approach

1. **External Perspective**: Our system primarily assesses an organization's security posture from an external perspective. While this allows for non-intrusive evaluation, it may not capture all internal security measures and practices.

   Consideration: Organizations should complement our external assessment with internal security audits and penetration testing for a comprehensive view of their security posture.

2. **Point-in-Time Assessment**: The cybersecurity landscape is constantly evolving, and our scores represent a snapshot at a specific point in time.

   Consideration: Regular reassessments are crucial to maintain an up-to-date understanding of an organization's security posture.

3. **Reliance on Public Data**: Our system relies heavily on publicly available data and external scanning. This means we may miss vulnerabilities or security measures that are not externally visible.

   Consideration: Organizations should be aware that their internal security practices, which may be robust, might not be fully reflected in the Score.

4. **Limited Context**: Our automated system cannot fully understand the unique context of each organization, such as specific business requirements or risk tolerances.

   Consideration: Scores should be interpreted in the context of the organization's specific circumstances and risk tolerance.

5. **Evolving Threat Landscape**: New types of cyber threats emerge constantly, and our system may not immediately account for novel attack vectors.

   Consideration: Organizations should stay informed about emerging threats and not rely solely on our Scores for threat intelligence.

Potential Biases

1. **Size Bias**: Despite our efforts to normalize the Scores based on organization size, there may still be some inherent advantages or disadvantages for organizations of certain sizes.

Consideration: When comparing the Scores, it's most meaningful to compare organizations of similar size and complexity.

2. **Industry Bias**: Some industries may consistently score higher or lower due to sector-specific technologies or regulations, rather than actual security effectiveness.

   Consideration: the Scores are most useful when compared within the same industry or to track an individual organization's progress over time.

3. **Technology Bias**: Our scanning and assessment techniques may be more effective for certain technologies or platforms, potentially leading to more accurate Scores for organizations using these technologies.

   Consideration: Organizations using less common or proprietary technologies should be aware that their Scores might not be as comprehensive.

Incomplete Picture

1. **Human Factor**: Our system cannot directly assess human factors such as security awareness or adherence to policies, which are crucial aspects of an organization's overall security.

   Consideration: Organizations should complement our technical assessments with evaluations of their security culture and employee practices.

2. **Compensating Controls**: Organizations may have compensating controls in place that mitigate risks identified by our system, but these may not be visible to our external scans.

   Consideration: Users of our system should be prepared to contextualize the Scores with information about their internal security measures.

3. **Data Accuracy**: While we strive for accuracy, the data we collect may sometimes be incomplete or slightly outdated due to the dynamic nature of the internet and the lag in updating certain public databases.

   Consideration: Organizations should verify critical findings and not treat the Scores as absolute truths.

4. **Passive Scanning:** Due to legal limitations, we may evaluate an organization only through means of passive scanning, which may give false positives and/or incomplete picture of security posture, thus there is a possibility for the data to contain some inaccuracies.

Mitigation Strategies

To address these limitations, we employ several strategies:

1. **Continuous Improvement**: We regularly update our scanning techniques and scoring algorithms to account for new threats and technologies.

2. **Multiple Data Sources**: By using a variety of data sources, we aim to create a more complete picture of an organization's security posture.

3. **Transparency**: We are open about our Scoring methodology and its limitations, allowing users to make informed decisions about how to interpret and act on our Scores.

4. **Contextual Guidance**: We provide guidance on how to interpret the Scores in different contexts and emphasize the importance of combining our assessments with internal security practices.

5. **Regular Calibration**: We periodically calibrate our Scoring system against real-world security incidents to ensure it remains predictive and relevant.

Conclusion

While our Scoring system provides valuable insights, it's important to recognize that no automated system can provide a perfect assessment of an organization's cybersecurity posture. Our Scores should be used as one tool among many in a comprehensive security strategy.

Organizations should use these Scores as a starting point for deeper investigation, combine them with internal assessments, and always consider their unique context when interpreting results. By understanding these limitations and considerations, users of our system can make more informed decisions about their cybersecurity strategies and investments.