BITSIGHT

REPORT

Implied Cyber Threat Methodology

Methodology Overview

Bitsight was founded with the goal of increasing transparency about cybersecurity, enabling dynamic, informed interactions between global market participants and incentivizing a more trustworthy and secure global ecosystem.

- We are committed to creating trustworthy, data-driven, and dynamic measurements of organizational cybersecurity performance and being transparent about our processes and methodology.
- In this article, we'll describe Bitsight's new Implied Cyber Threat analytic and detail how this analytic enables us to continue to push forward this vision.

IMPLIED CYBER THREAT ANALYTIC:

Objectives

Over the next two years, the World Economic Forum lists cybersecurity risk as a greater threat to organizations than the risk of economic downturn, geopolitical conflict, and inflation.[1] Considering this increasing threat to the global economy—cyber risk must be a key consideration across all risk management practices, processes and decisions to facilitate operational and financial resiliency. These practices include lending, customer diligence, insurance underwriting and investing where cyber events continue to impact firm performance, business resilience and downside risk.

Addressing the needs of risk managers requires visibility into the cyber risk posed by the extended business ecosystem, not just third parties with access to critical digital infrastructure. This in turn necessitates a cyber assessment criteria for the long tail, including organizations where cyber risk is typically not considered due to their size, function, maturity or complexity. Furthermore, this insight must be digestible, actionable and meaningful for risk practitioners who are not cyber risk experts but rather cyber risk consumers in need of a cyber input into a larger third-party risk assessment criteria.

The Implied Cyber Threat analytic by Bitsight is a next-gen firmographic-based cyber analytic that addresses these key requirements. Built upon Bitsight's leading cyber risk analytics engine, the Implied Cyber Threat analytic provides cyber risk insight into over 325 million organizations globally.

In accordance with our guiding principle of Empiricism, the Implied Cyber Threat analytic is not only based on objective, verifiable data, but it is correlated with real-world outcomes.

- Addressing the needs of risk managers requires visibility into the cyber risk posed by the extended business ecosystem, not just third parties with access to critical digital infrastructure.

[1] *https://www.weforum.org/agenda/2024/01/global-risk-report-2024-risks-are-growing-but-theres-hope/#:~:text=Among%20the%20top%20risks%20are,the%20World%20Economic%20Forum%20explain.*

IMPLIED CYBER THREAT ANALYTIC:

Definition

The Implied Cyber Threat analytic is Bitsight's analysis of the inherent risk that a given organization faces based on:

1. Firmographic attributes

2. Implied technographic attributes

Together, the firmographic and technographic metrics create a single, succinct analytic that identifies potential risks and their potential negative impacts. Risk practitioners can utilize this analysis as a component of overall business risk modeling.

The Implied Cyber Threat analytic quantifies the inherent risk of an organization based on firmographic business factors — **size, sector,** and **country**, on a five-category scale: Very Low Risk, Low Risk, Medium Risk, High Risk, and Very High Risk. Higher-risk cohorts are increasingly likely to be impacted by a cybersecurity event. Risk categories are evenly distributed across the covered companies, with each of the five Implied Cyber Threat analytic categories mapping to approximately 20% of organizations, providing a comparative view of risk across individual companies.

The Implied Cyber Threat analytic is calculated for over 600,000 unique firmographic business cohorts to maximize its correlation to bad cyber outcomes such as data breaches and ransomware events. These cohorts are built on top of the industry-leading Moody's Orbis firmographic dataset. As of March 2024, the Implied Cyber Threat analytic is available for over 325 million entities.

Firmographic Business Factors

These factors inform the likelihood of both cyber attack targeting and an organization's ability to withstand an attack.

- **Company Size**
  Size is determined based on operating revenue, total assets and employee count.
- **Company Size**
  Sector is determined by NACE code. NACE (Nomenclature des Activités Économiques dans la Communauté Européenne) is a European industry standard classification system similar in function to Standard Industry Classification (SIC) and North American Industry Classification Systems (NAICS) for classifying business activities.
- **Country**
  Country is determined by ISO country code.

+

Bitsight Technographic Data

These risk vectors are proven to correlate to adverse cybersecurity outcomes, including data breaches and ransomware attacks

- **Botnet Infections**
  Botnets can be used to exfiltrate corporate secrets and sensitive customer information, repurpose company resources for illegal activities, and serve as conduits for other infections.
- **Potentially Exploited Systems**
  Devices observed to be running potentially malicious or unwanted software are often indicative of other infections and reflect insufficient device controls.
- **TLS / SSL Certificates**
  Certificates should effectively encrypt traffic over the Internet.
- **TLS / SSL Configurations**
  Configurations should support strong encryption standards when making encrypted connections to other machines.
- **Open Ports**
  Unnecessary open ports provide ways for attackers to access a company's network.

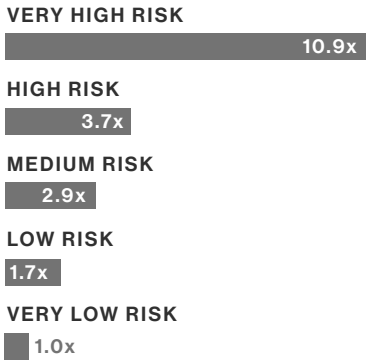
=

Implied Cyber Threat Analytics

Quantification of an organization's inherent cyber risk and probability of a cybersecurity incident based on business profile

Five-Category Scale
Higher-risk cohorts are increasingly likely to be impacted by a cybersecurity event

Likelihood of Cybersecurity Incident
vs. Very Low Risk category

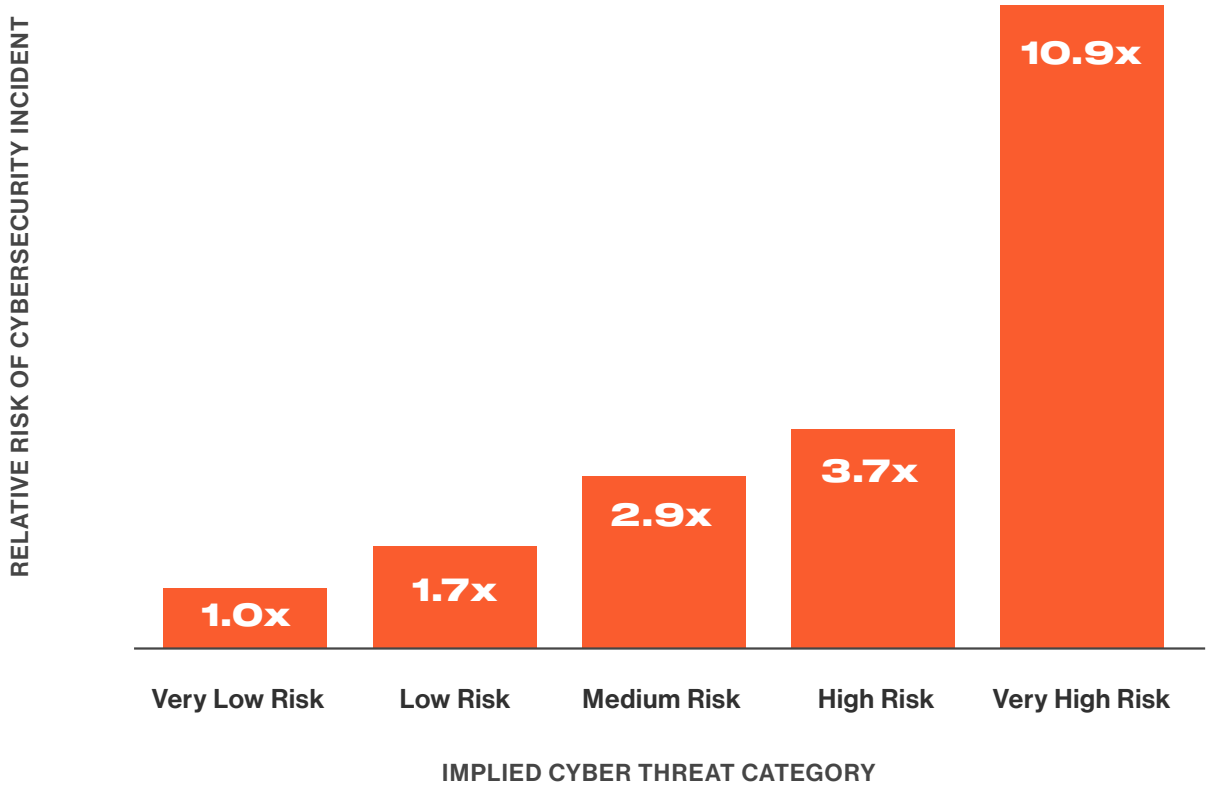


600k+ Firmographic Cohorts
That are then mapped to...

325M+ Unique Organizations

The Implied Cyber Threat analytic is based on objective, verifiable data, and it is correlated with real-world outcomes.

LIKELIHOOD OF CYBERSECURITY INCIDENT
vs. Very Low Risk category



Bitsight maintains one of the largest proprietary databases of publicly disclosed cybersecurity incidents in the industry. We collect information on data breaches and other cybersecurity incidents from a large number of verifiable sources; e.g. reputable news organizations and regulatory reporting (obtained via Freedom of Information Act requests or local analogs). Each incident is assigned a severity score based on incident type (ransomware, espionage, phishing, etc) and the number of records of personal information involved, adjusted for company size. Learn more

We utilize this expansive dataset to train and validate our Implied Cyber Threat analytic model. As a result, the model output represents the inherent probability of a cybersecurity incident associated with an organization's business profile.

This highly correlated cyber risk signal enables risk managers to confidently assess, benchmark, and act against cyber risk to reduce exposure across the broader business ecosystem.

The Implied Cyber Threat analytic can be utilized as a:

- Complementary measure of systematic risk across cohorts
- Comparable analytic with unrated entities, where a Bitsight security rating exists
- Standalone, comparable cyber risk measure (likelihood of material events), where a Bitsight security rating does not exist

For example, if an organization is assessing cyber security when evaluating a set of companies to acquire, they can filter out certain cohorts based on their potential for downside cyber risk. Let's consider the following scenarios:

SCENARIO A

An organization is considering acquiring a new business to bolster its manufacturing operations. When evaluating the new businesses, cohort A has an Implied Cyber Threat of "Low Risk" and cohort B has an Implied Cyber Threat of "Very High Risk." Depending on the risk appetite of the acquiring organization, they may decide that the heightened Implied Cyber Threat to cohort B does not outweigh the potential upside for their manufacturing capabilities.

SCENARIO B

Additionally, if a critical supplier is operating in a "Very High Risk" Implied Cyber Threat environment, indicating a higher likelihood of impactful cyberattack, an organization may consider securing a redundant supplier to minimize operational disruption in the event of a cybersecurity incident.

SCENARIO C

Similarly, if the Implied Cyber Threat analytic of a financial counterparty is "Medium Risk" or higher, an organization may consider requiring proof of cyber insurance to minimize downside risk in the event of a cybersecurity incident.

SCENARIO D

Because it is calculated based on firmographic factors, the Implied Cyber Threat analytic can also be deployed to assess inherent business risk and prioritize mitigation efforts as part of the enhanced due diligence process.

To be clear, the Implied Cyber Threat analytic is not a Bitsight security rating substitute. It is designed to provide insight into the cyber risk inherent to an operating environment, based on business characteristics to support business conversations and business decisioning through context. It is not intended to measure or represent the cybersecurity performance of a specific entity against an array of security controls or best practices.

Cyber risk thresholds may vary based on the nature of an organization's relationship with a member of your business ecosystem. Business context is an important factor to consider when evaluating cyber risk tolerance and the level of cybersecurity evaluation required. We recommend organizations consult with their Information Security teams to determine the appropriate Implied Cyber Threat analytic thresholds and associated cybersecurity diligence requirements for various types of business relationships.

In the event a member of your business ecosystem fails to meet the minimum Implied Cyber Threat analytic threshold, we suggest engaging with that organization to learn more about their cybersecurity program or adding compensating defenses necessary to ensure the resiliency where necessary for your business. In addition to reviewing their Bitsight security rating, diligence may include solicitation for the company's information security policy, SOC 2 report, and other documentation.

IMPLIED CYBER THREAT ANALYTIC:

Principles

Bitsight is committed to creating trustworthy, data-driven, and dynamic measurements of organizational cybersecurity performance derived from objective, verifiable information. As the framework for creating the methodology behind our security ratings, Bitsight uses the US Chamber of Commerce's Principles for Fair and Accurate Security Ratings, which we helped develop:

- Transparency
- Dispute, Correction and Appeal
- Accuracy and Validation
- Model Governance
- Independence
- Confidentiality

Learn more →

Furthermore, Bitsight uses these additional guidelines when considering how to build our security rating & cyber risk analytics' models and governance practices:

Comparability.
Implied Cyber Threat analytic categories must allow meaningful comparisons of inherent cyber risk between organizations.

Ubiquity.
Implied Cyber Threat analytic categories should be readily available for large numbers of organizations, in all industries, and across the world. This enables comparison against industry and global benchmarks.

Empiricism.
Implied Cyber Threat analytic categories should be based on objective, verifiable data, rather than opinion or subjective judgments. They should be correlated with real-world outcomes.

Stability.
Implied Cyber Threat analytic categories should be relatively stable (free from spurious fluctuations).

IMPLIED CYBER THREAT ANALYTIC:

Rating Process

The Implied Cyber Threat analytic is built upon multiple dimensions of the Bitsight security rating. To produce these analytics Bitsight continuously measures the security performance of organizations based on evidence of compromised systems, cybersecurity hygiene, and publicly disclosed security incidents to provide an objective, evidence-based measure of performance.

These analytics are built on data from over 100 different data sources. Bitsight collects much of the data ourselves, and we also work with numerous best-in-class data partners (many exclusive) who specialize in various types of telemetry. To date, Bitsight has collected petabytes of security-relevant data and adds billions of new observations daily. We use a combination of human and machine intelligence to screen out false positives and to ensure that the data we process is accurate.

Bitsight data is independently verified to correlate with an organization's risk of a security incident or data breach. See reports by Marsh McLennan, Moody's Analytics, AIR Worldwide and IHS Markit demonstrating this critical connection.

While all of our data is collected externally, from the Internet (vs. internal networks), that's not to say that our data sources are all public. Much of what we observe relies on sophisticated and proprietary techniques and infrastructure, which differentiate us from others in this space.

Bitsight does not conduct penetration testing or any other intrusive activity, nor does it require permission or information from an organization, to produce its security rating. This external perspective enables us to rate hundreds of thousands of organizations worldwide and also allows us to maintain independence and objectivity.

Each observation has potential implications for an organization's security posture. To assess this, observations are first processed into a set of risk vectors, each of which measures a particular area of security performance.

What we learn by listening

We have an extensive network of sensors deployed at key locations across the internet. With these, we can see:

- Communications from comprised systems
- DNS queries and responses
- Malicious traffic; e.g. DDOS attacks
- Attempats at brute force attacks
- File sharing
- Endpoint device identifiers
- Traffic from IOT devices
- BGP announcements

What we learn by actively looking

We use non-intrusive probes and queries to observe:

- Open ports
- Server software, configuration and versions
- Known vulnerabilities (CVEs)
- DNS records, including SPF and DKIM
- Web applications

The Implied Cyber Threat analytic leverages Bitsight analytics from three categories of security data - Compromised Systems, Diligence, and Public Disclosures.

Comprised Systems:

Compromised Systems are devices or machines in an organization's network that show symptoms of malicious or unwanted software. These compromises can disrupt daily business operations and can increase an organization's risk of breach.

Compromised Systems are evaluated based on the number and type of malware, the severity, and the duration.

Learn more →

Diligence:

Diligence risk vectors show steps a company has taken to prevent attacks. Bitsight currently evaluates SPF, DKIM, TLS/SSL, Open Port and DNSSEC information in assessing a company's security diligence.

All diligence records are evaluated as one of the following: Good, Fair, Warn, Bad or Neutral. Records are assessed using industry-standard criteria.

Learn more →

Public Disclosures:

Public Disclosure events provide information on breaches, general security incidents, and other disclosures related to possible incidents of undesirable access to a company's data.

Learn more →

The Implied Cyber Threat analytic is built on normalized, country-level aggregates of forensic cybersecurity findings mapped to select Bitsight risk vectors:

Comprised Systems:

- **Botnet Infections:** Devices observed participating in botnets as either bots or Command and Control servers. Botnets can be used to exfiltrate corporate secrets and sensitive customer information, repurpose company resources for illegal activities, and serve as conduits for other infections. Botnet detections are detected by capturing traffic from malicious software, using techniques such as sinkholing. Learn more →
- **Potentially Exploited Systems:** Devices observed to be running potentially malicious or unwanted software; e.g. greyware or adware. These events are often indicative of other infections, and, like botnet infections, reflect insufficient device controls. Learn more →

Diligence:

- **TLS/SSL Certificates:** TLS/SSL certificates are used to encrypt traffic over the Internet. Bitsight analyzes certificates and provides information about their effectiveness; e.g. whether they are signed using a secure algorithm. Learn more →
- **TLS/SSL Configurations:** Evaluates whether servers have correctly configured security protocol libraries, and support strong encryption standards when making encrypted connections to other machines. Learn more →
- **Open Ports:** Which port numbers and services are exposed to the Internet. Certain ports must be open to support normal business functions; however, unnecessary open ports provide ways for attackers to access a company's network. Learn more →

These risk vectors were selected as model inputs based on a number of criteria, including proven correlation to adverse cyber security outcomes in other studies. The relationship between these inputs and bad outcomes may change over time. In order to maintain this correlation, Bitsight will reevaluate the Implied Cyber Threat analytic modeling framework, including model inputs, on an annual cadence.

Leveraging market leading firmographic data from the Moody's Orbis database, Bitsight utilizes these risk vectors to produce the Implied Cyber Threat analytics for over 600K unique cohorts based on combinations of entity size, sector and geographic location.

Size:

The size of an organization is closely correlated with cyber attack surface size and willingness to pay ransom. Each of these factors can inform the likelihood of cyberattack targeting.

Size is determined based on operating revenue, total assets and employee count.

According to the Verizon Data Breach Investigations Report, financial motives still drive the vast majority of breaches. Larger organizations are increasingly targeted by ransomware attackers, due to their perceived willingness to pay large sums to avoid the operational disruption and reputational consequences of a prolonged ransomware attack.

Orbis Firmographic Attribute:
Company Category, Size Classification

Geographic Location:

Geographic cyber risk factors include regulatory environment, geopolitical climate and corruption levels. Each of these location-specific features can inform the likelihood of cyberattack targeting.

Country is determined by ISO country code.

As a result of the ongoing war in Ukraine, organizations in the region are operating in an elevated cyber risk environment due to increased targeting from geopolitical adversaries. According to the CyberPeace Institute, over 600 cyberattacks have been launched against Ukrainian based entities since the war began.

Orbis Firmographic Attribute:
Country ISO Code

Sector:

Attitudes about cybersecurity risk, expertise in cybersecurity risk mitigation, and IT spending vary across different industries. Further, the relative value of one industry's data over another, or the relative importance to society of one industry over another, can inform the likelihood of cyberattack targeting.

Sector is determined by NACE code. NACE (Nomenclature des Activités Économiques dans la Communauté Européenne) is a European industry standard classification system similar in function to Standard Industry Classification (SIC) and North American Industry Classification System (NAICS) for classifying business activities.

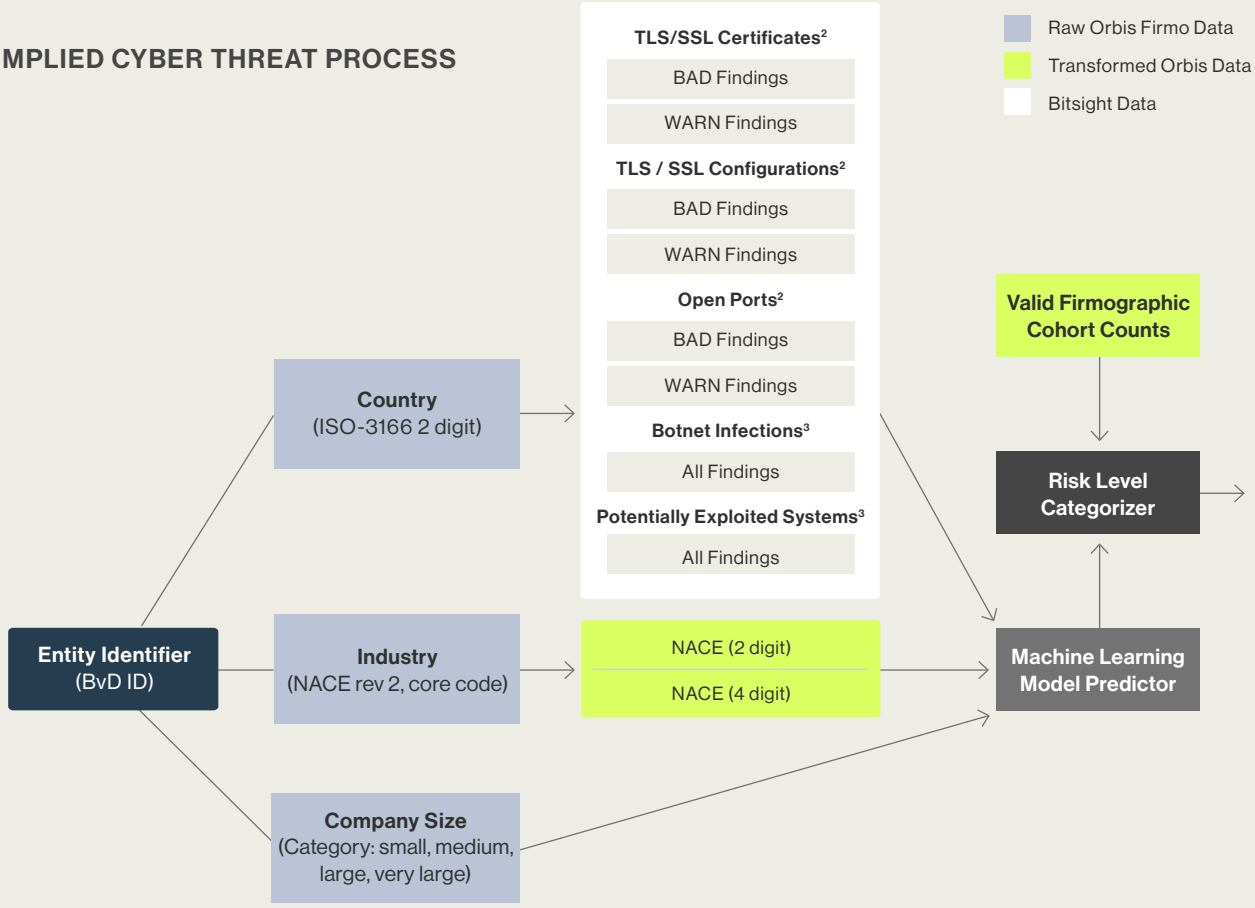
Because they are highly regulated, financial institutions tend to invest heavily in cybersecurity. They are also heavily targeted by attackers due to their valuable data assets such as clients' personal data and commercial information, as well as payment card numbers and account details. Per the Verizon Data Breach Investigations Report, the finance industry notched the highest number of incidents with confirmed data disclosure.

Orbis Firmographic Attribute:
NACE Rev. 2, Core Code (4 digits)

In total, eleven cyber risk categorical firmographic features and technographic cyber risk country-level continuous features are utilized to calculate the Implied Cyber Threat analytic for a given size / sector / geographic cohort.

Bitsight cyber risk analytics leverage historical technographic findings to quantify inherent risk over time. Specifically, the Implied Cyber Threat analytic as of a given date is based on forensic-level observations and findings collected over the prior 60-day period.

THE IMPLIED CYBER THREAT PROCESS



² Normalized by total number of findings for each country
³ Normalized by estimated number of internet users in a country

IMPLIED CYBER THREAT ANALYTIC:

Maintenance and Algorithmic Adjustments

The Implied Cyber Threat will be computed monthly and the underlying model will be retrained quarterly.

On an annual basis we will review the Implied Cyber Threat analytic methodology and consider potential algorithmic improvements including hyperparameter tuning, predictors, and overall modeling framework.