

REPORT

# Make better cybersecurity decisions with trusted data analytics

Marsh McLennan study finds statistically significant correlation between Bitsight analytics and cybersecurity incidents

# Executive summary

The Marsh McLennan Cyber Risk Analytics Center (Marsh McLennan) analyzed Bitsight's cybersecurity performance data to consider its potential benefits for market participants in helping to prioritize resources, address security risks, lower the probability of experiencing a cybersecurity incident, reduce insurance claims, and improve the cyber insurance underwriting and acquisition process.

After comparing the security performance data of thousands of organizations that experienced cybersecurity incidents against those that did not, Marsh McLennan identified 14 Bitsight analytics, including the Bitsight Security Rating and 13 risk vectors, that had statistically significant correlation to reported cybersecurity incidents.

These findings provide actionable insights to help cybersecurity and cyber risk stakeholders focus on which aspects of their organization's security processes need improvement, and inform resource allocation, programmatic decision-making, and cyber insurance underwriting.

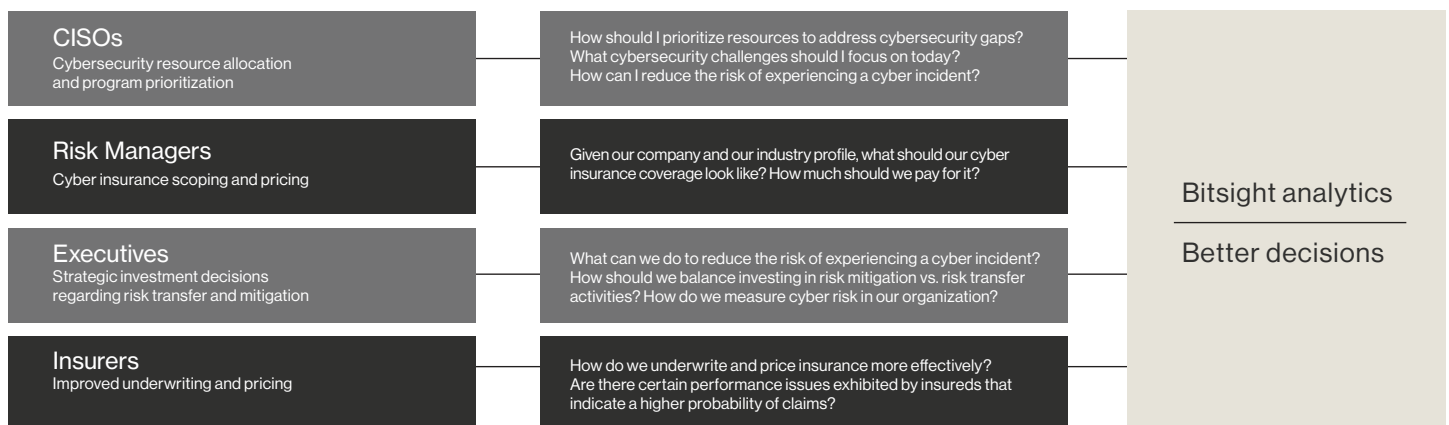
## Background

Cybersecurity continues to be a top risk for business and government leaders worldwide. Malicious actors continue to find new, innovative methods to harm organizations. The onslaught continues, from creating highly sophisticated phishing campaigns to conducting far-reaching supply chain attacks to exploiting new vulnerabilities across the rapidly expanding universe of software and Internet of Things (IoT) devices. In recent years, ransomware has emerged as a serious threat to organizations of all sizes and sectors, resulting in soaring financial costs and frequent operational disruptions.

The need for trusted data that better enables cybersecurity decision-making and reduces the likelihood of incidents is more critical than ever as security, business, and financial leaders on the front lines are facing significant challenges in addressing these risks.

### Stakeholders & challenges

### Questions



Each market participant needs quantitative, objective, trusted data and insights regarding cybersecurity program performance to help them make better, more confident decisions. In cybersecurity, a lack of objective, quantitative, and transparent data tied to specific outcomes (e.g. cyber incidents) has limited the ability for market participants to act with greater confidence.

Marsh McLennan's independent analysis of Bitsight's analytics and risk vectors can help market participants:

- Prioritize resources and address security risks.
- Lower the probability of experiencing a cybersecurity incident.
- Improve cyber insurance coverage with better security performance.
- Improve the cyber insurance underwriting and acquisition process.

## Key findings

Marsh McLennan identified 14 Bitsight analytics to be statistically significant and correlated with cybersecurity incidents, including the Bitsight Security Rating and 13 risk vectors. Bitsight's Patching Cadence risk vector, which measures the rate at which organizations remediate important vulnerabilities, was most strongly correlated to cybersecurity incidents, followed by risk vectors that measure updated desktop and mobile software and observed exploited devices.

Marsh McLennan concluded that poor performance in these areas increased an organization's risk of experiencing a cybersecurity incident, while strong performance implied a lower risk of incident. Market participants should pay particularly close attention to key findings in these areas when forming a strategy to avoid cybersecurity incidents. A detailed statistical analysis is separately available for readers interested in learning more.

## The top14

14 Bitsight Analytics are clearly correlated with the risk of facing a cybersecurity incident

- |   |                                      |
|---|--------------------------------------|
| <b>01</b> Bitsight Security Rating      | <b>08</b> Web Application Headers    |
| <b>02</b> Patching Cadence              | <b>09</b> User Behavior              |
| <b>03</b> Desktop Software              | <b>10</b> TLS/SSL Configurations     |
| <b>04</b> Potentially Exploited Systems | <b>11</b> Open Ports                 |
| <b>05</b> Mobile Software               | <b>12</b> TLS/SSL Certificates       |
| <b>06</b> Botnet Infections             | <b>13</b> Spam Propagation           |
| <b>07</b> Insecure Systems              | <b>14</b> Unsolicited Communications |

The following Bitsight analytics were identified to be statistically significant and correlated with cybersecurity incidents:

**01** Bitsight Security Rating

Measures an organization's cybersecurity performance – how effective it is in preventing cybersecurity incidents.

**02** Patching Cadence

Measures how many systems within an organization's network are affected by important vulnerabilities, and how quickly the organization remediates them.

**03** Desktop Software

Measures whether browser and operating system versions are kept up-to-date for laptops, servers, and other non-tablet, non-phone computers in an organization's network with access to the Internet.

**04** Potentially Exploited Systems

Measures devices observed to be running potentially malicious or unwanted programs or software (e.g. greyware or adware).

**05** Mobile Software

Measures whether mobile software and associated devices such as phones and tablets are kept up-to-date.

**06** Botnet Infections

Measures devices on an organization's network observed participating in botnets as either bots or Command and Control servers.

**07** Insecure Systems

Measures endpoints communicating with an unintended destination. Software on these endpoints may be outdated, tampered with, or misconfigured.

**08** Web Application Headers

Measures web server traffic by examining security-related fields in the header section of HTTP request and response messages.

**09** User Behavior

Measures how often employees at an organization are observed engaging in potentially risky behaviors, including sharing files using peer-to-peer networks (e.g. BitTorrent).

**10** TLS/SSL Configurations

Measures whether an organization has correctly configured security encryption software, and whether that software utilizes strong encryption protocols when making encrypted connections to other machines.

**11** Open Ports

Measures which port numbers and services are exposed to the Internet.

**12** TLS/SSL Certificates

Measures whether an organization has properly obtained and deployed TLS/SSL encryption certificates that are used to secure communication over the Internet.

**13** Spam Propagation

Measures if an organization is infected with malware and sending unsolicited commercial or bulk email (spam).

**14** Unsolicited Communications

Measures if an organization's devices are seeking to contact a service that is unexpected, unsupported, or not useful on another network, indicating that they may be compromised.

# Recommendations for market professionals

Prioritize resources and address security risks.

- Leverage this analysis to prioritize programmatic efforts and investment to reduce your organization's risk of experiencing a cybersecurity incident.

Lower the probability of experiencing a cybersecurity incident.

- Address critical findings in prioritized Bitsight risk vectors and determine if there are underlying programmatic areas that could lead to weaknesses in these risk vectors.

## Security program area



Vulnerability  
Management



Endpoint Protection  
& Malware Detection



Secure  
Communications



User Training &  
Awareness

## Bitsight risk vectors

### 01.

Patching Cadence  
Desktop Software  
Mobile Software

### 02.

Potentially Exploited Systems  
Botnet Infections  
Insecure Systems  
Open Ports  
User Behavior  
Spam Propagation  
Unsolicited Communications

### 03.

Web Application Headers  
TLS/SSL Configurations  
TLS/SSL Certificates

### 04.

User Behavior  
Botnet Infections  
Potentially Exploited

Source: Bitsight

- Focus on these key risk vectors when assessing the security performance of your third-party ecosystem. Vendors with poor performance across these risk vectors may be at a heightened risk of cybersecurity incidents.

Improve cyber insurance coverage with better security performance.

- Focus your cyber insurance discussions with carriers on the Bitsight analytics that were covered in this analysis to make those efforts more productive and efficient.
- Showcase the effectiveness of your organization's security performance in these areas to negotiate better insurance coverage for your organization. Bitsight data is used by insurers who collectively underwrite more than 50% of cyber insurance premiums globally.

## Improve the cyber insurance underwriting and acquisition process.

- Focus risk selection and loss prevention efforts on the Bitsight analytics that are most highly correlated with cybersecurity incidents.

### About the Study:

The Marsh McLennan Cyber Risk Analytics Center conducted an independent analysis of Bitsight's data analytics (Security Rating and risk vectors) and Marsh McLennan's reported cybersecurity incident data.

Marsh McLennan leveraged proprietary and licensed cyber claims and incident data for the analysis. Marsh McLennan collects cybersecurity incidents and claims data from thousands of organizations in its customer portfolio. Reports are submitted when an organization has experienced a cyber incident. For purposes of this study, a cybersecurity incident was defined as a malicious attack (e.g. ransomware, business interruption, data breach) resulting in an insurance notification or claim that was logged in Marsh McLennan's proprietary database from 2018 to 2021. The study was conducted without providing Bitsight access to Marsh McLennan's data.

Bitsight provided Marsh McLennan cybersecurity performance data across 365,000 organizations to conduct this study. Bitsight non-intrusively collects unique telemetry into the cybersecurity performance of organizations around the globe, and uses it to create analytics that measure performance over time. The Bitsight Security Rating measures an organization's overall cybersecurity performance. Bitsight risk vectors measure an organization's performance in particular cybersecurity domains (e.g. patching cadence, software updating practices, etc.).

This document and any recommendations, analysis, or advice provided by Marsh McLennan are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. This document and any recommendations, analysis or advice provided herein (i) are based on our experience as insurance and reinsurance brokers or as consultants, as applicable, (ii) are not intended to be taken as advice or recommendations regarding any individual situation, (iii) should not be relied upon as investment, tax, accounting, actuarial, regulatory or legal advice regarding any individual situation or as a substitute for consultation with professional consultants or accountants or with professional tax, legal, actuarial or financial advisors, and (iv) do not provide an opinion regarding the fairness of any transaction to any party.

The opinions expressed herein are valid only for the purpose stated herein and as of the date hereof. We are not responsible for the consequences of any unauthorized use of this report. Its content may not be modified or incorporated into or used in other material, or sold or otherwise provided, in whole or in part, to any other person or entity, without our written permission. No obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof. Information furnished by others, as well as public information and industry and statistical data, upon which all or portions of this report may be based, are believed to be reliable but have not been verified. Any modeling, analytics or projections are subject to inherent uncertainty, and any opinions, recommendations, analysis or advice provided herein could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. We have used what we believe are reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied, and we disclaim any responsibility for such information or analysis or to update the information or analysis in this report. We accept no liability for any loss arising from any action taken or refrained from, or any decision made, as a result of or reliance upon anything contained in this report or any reports or sources of information referred to herein, or for actual results or future events or any damages of any kind, including without limitation direct, indirect, consequential, exemplary, special or other damages, even if advised of the possibility of such damages. This report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. No responsibility is taken for changes in market conditions or laws or regulations which occur subsequent to the date hereof.

Bitsight transforms how companies manage information security risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of external data on security issues. Seven of the largest 10 cyber insurers, 80 Fortune 500 companies, and 3 of the top 5 investment banks rely on Bitsight to manage cyber risks.

BOSTON (HQ)

RALEIGH

LISBON

SINGAPORE

BUENOS AIRES



**BITSIGHT**