BITSIGHT

ACADEMIC PAPER

Quantifying relationships between cybersecurity performance and likelihood of cybersecurity incidents

A Marsh McLennan cyber risk analytics center study of Bitsight cybersecurity analytics

Table of Contents

Introduction

Many have struggled to establish a data-driven relationship between poor cybersecurity performance and the increased likelihood of experiencing cybersecurity incidents. Decisions regarding risk acceptance, mitigation, and transfer are often qualitative and based primarily on expert judgment.

Market professionals can benefit from cyber risk analytics that demonstrate strong correlations with cybersecurity incidents such as data breach and ransomware. With trusted, proven, objective analytics:

- Business executives and security professionals can follow an established path to both improve their organizations' security posture and more effectively acquire cyber insurance coverage;
- Investors can better monitor the security posture of their portfolio companies;
- Insurers can better understand their aggregate exposure, reduce the potential for losses, and better price policies; and
- Regulators and government officials can make more informed policy decisions and perform better cybersecurity oversight.

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. Because Bitsight's cybersecurity performance data is collected continuously and non-intrusively, it provides an independent, objective view of an organization's cybersecurity performance.

Marsh McLennan sought to quantify the relationship between Bitsight's data analytics and Marsh McLennan's cybersecurity incident data. After comparing the security performance data of thousands of organizations that experienced cybersecurity incidents against those that did not, Marsh McLennan found many Bitsight analytics to be statistically signficant and correlated with cybersecurity incidents, including the Bitsight Security Rating and various risk vectors. Marsh McLennan concluded that deficiencies in these performance areas increased an organization's risk of experiencing a cybersecurity incident, while strong performance implied a lower risk of incident.

In this paper, we will review Marsh McLennan's findings and recommend how the market can leverage these findings to make better cyber risk decisions.

Data and Methodology

Bitsight shared a proprietary cybersecurity performance data set with Marsh McLennan so data scientists at the Marsh McLennan Cyber Risk Analytics Center could ascertain which Bitsight cyber risk analytics, if any, were most correlated with the likelihood of a cybersecurity incident. These analytics–including Bitsight Security Ratings and risk vectors–provided a uniform set of measurements across all companies in the data set and are described in further detail throughout this paper. Bitsight provided Marsh McLennan with a data set that included Security Ratings and risk vectors for 365,000 organizations.

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.

Combining the data sets, Marsh McLennan identified 14 analytics, including the Bitsight Security Rating and 13 Bitsight risk vectors, that had a statistically signficant correlation to reported cybersecurity incidents for Marsh McLennan clients. The study was conducted by Marsh McLennan without providing Bitsight access to its data.

Analysis Methodology

To analyze this data, Marsh McLennan matched companies in the Bitsight inventory to companies that had purchased cyber insurance policies via Marsh McLennan. For each matched company, Marsh McLennan counted the number of cybersecurity incidents for each year from 2018 to 2021. The study looked at 12,000 unique organizations during the time period. Many organizations were evaluated in multiple years. Overall there were almost 16,000 company-years studied and the cybersecurity incident rate was 2.35 percent.

By comparing Marsh McLennan's annual incident data to the Bitsight Security Ratings and risk vector scores measured at the beginning of each year, it was possible to estimate the predictive power of the Bitsight Security Rating and risk vectors. To understand the correlation between Bitsight analytics and cybersecurity incidents, Marsh McLennan computed Rank-Biserial Correlation Coefficients. This metric uses performance ranks for victim and non-victim companies to determine how well Bitsight analytics correlated with the likelihood of a cybersecurity incident. The value of Rank-Biserial Correlation ranged between 1 (perfect correlation) and -1 (perfectly anti-correlated). Since we expected that lower performance was correlated with increased risk, we expected negative values for this metric.

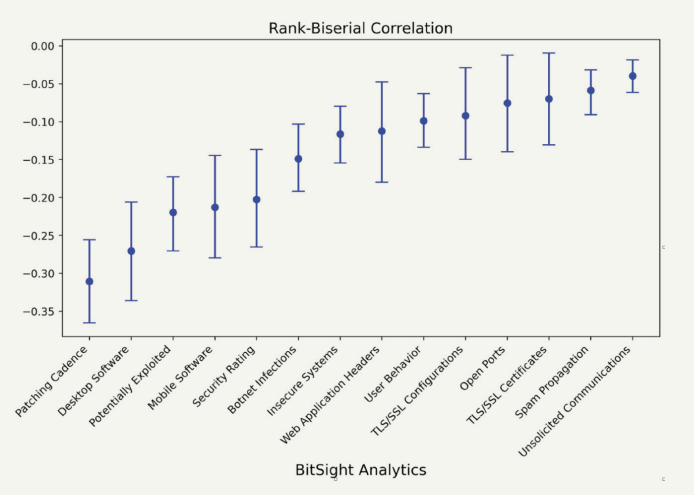
The Rank-Biserial Correlation was computed for each Bitsight risk vector and for the overall Security Rating. 95 percent confidence intervals were estimated for each correlation coefficient. This statistic was useful for determining the statistical significance and the overall amount of correlation, but it did not provide an easily interpretable risk metric. To facilitate easier interpretation, we reported relative risk as a function of the overall Security Rating. For each risk vector, we reported relative risk as a function of the risk vector grade.

Key Findings

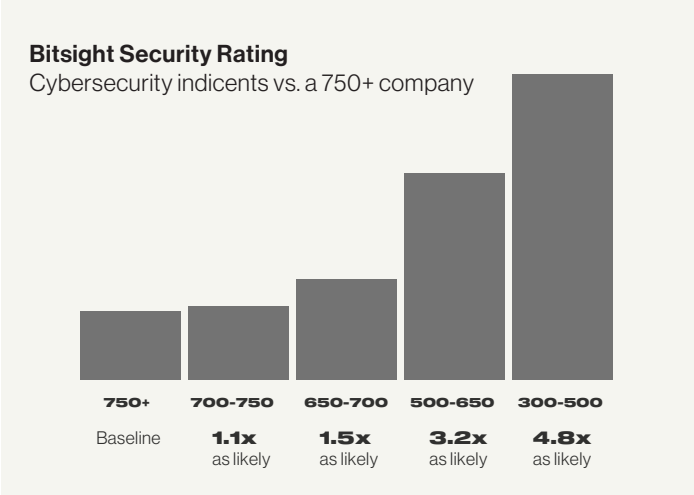
After comparing the security performance data of organizations that experienced cybersecurity incidents against those that did not, Marsh McLennan found many Bitsight analytics to be statistically signficant and correlated with cybersecurity incidents.

To summarize Marsh McLennan's primary findings, we present estimates of the Rank-Biserial Correlation for Bitsight's risk vectors and the relative risk as a function of the Security Rating.

The following plot shows the Rank-Biserial Correlation estimated for Bitsight's Security Rating and risk vectors. Statistically significant correlations were observed for 14 of Bitsight's analytics (the Security Rating and 13 risk vectors). We considered the correlation to be significant if the estimated value was negative and the upper end of the confidence interval was negative.



Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022



Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

The Rank-Biserial Correlation results showed that Patching Cadence, Desktop Software, Potentially Exploited, and Mobile Software were the most correlated with cybersecurity incidents. Many of these results are consistent with earlier Bitsight analyses (e.g. 2021 Bitsight research identified that poor performance in the Patching Cadence risk vector was known to be highly correlated with ransomware incidents).

The Rank-Biserial Correlation estimate for the Security Rating ranked fifth on this plot. The reason for this is that the most highly correlated risk vector components had a smaller contribution to the overall rating when compared with other more heavily weighted risk vectors. Bitsight plans to address this issue in upcoming updates to its Security Rating; using this study, in part, as a basis for future rating algorithm updates. Nonetheless, this analysis showed that the risk of a cybersecurity incident increased significantly as the overall rating dropped below 700 (see below chart). These results are statistically consistent with earlier results from a third-party analysis.

Risk vector correlations

To provide some context on the correlation results above, we showed the relative risk of a cybersecurity incident as a function of the Bitsight risk vector grade. Marsh McLennan's analysis demonstrated that there was a clear correlation between poor performance and increased risk of cybersecurity incidents.

The 13 risk vectors with measured correlation covered a diverse set of security program areas well known to security professionals, including Endpoint Management and Malware Detection, Vulnerability Management, Secure Communications, and User Training and Awareness. For these risk vectors, we saw that the relative risk peaks between 2 and 5. The strongest signals were for risk vectors associated with Endpoint Management, Malware Detection, and Vulnerability Management. Definitions and descriptions for each of the risk vectors is included in the Appendix.

In the table below, we show risk estimates where we often computed the average risk for a set of grades (e.g. D and F). The raw measurements (shown in the Appendix) sometimes showed fluctuating risk with worsening grades. We attributed those decreasing risk estimates to statistical uncertainties.

Correlation to Cybersecurity Incidents ↓

Risk vector	A	B	C	D	F
01. Patching Cadence	1.0	2.0	3.2	3.2	3.2
02. Desktop Software	1.0	1.5	2.0	2.7	2.9
03. Potentially Exploited	1.0	3.0	3.0	4.8	4.8
04. Mobile Software	1.0	1.6	2.1	2.1	2.1
05. Botnet Infections	1.0	2.0	2.7	3.4	4.1
06. Insecure Systems	1.0	2.3	2.5	4.1	4.2
07. Web Application Headers	1.0	1.1	1.1	1.1	2.5
08. User Behavior	1.0	3.5	3.5	3.5	3.5
09. TLS/SSL Configurations	1.0	1.4	1.4	1.6	2.2
10. Open Ports	1.0	2.0	2.0	2.0	2.0
11. TLS/SSL Certificates	1.0	1.6	1.6	1.6	1.6
12. Spam Propagation	1.0	2.9	2.9	2.9	2.9
13. Unsolicited Communications	1.0	4.2	4.2	4.2	4.2

Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

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

01.	02.	03.	04.
Vulnerability Management	Endpoint Protection & Malware Detection	Secure Communications	User Training & Awareness

Bitsight risk vectors

01.	02.	03.	04.
Patching Cadence	Potentially Exploited Systems	Web Application Headers	User Behavior
Desktop Software	Botnet Infections	TLS/SSL Configurations	Botnet Infections
Mobile Software	Insecure Systems	TLS/SSL Certificates	Potentially Exploited
	Open Ports		
	User Behavior		
	Spam Propagation		
	Unsolicited Communications		

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 Bits ight analytics that are most highly correlated with cybersecurity incidents.

Conclusion

This study demonstrated a statistically signficant correlation between Bitsight's data analytics and the likelihood of experiencing a cybersecurity incident, 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.

Marsh McLennan identified statistically significant correlations for 14 Bitsight cybersecurity analytics, including 13 of Bitsight's risk vectors and the overall Bitsight Security Rating. These results indicated that Bitsight's Security Rating can be used to effectively gauge the cyber risk of a company. The specific correlations found for different risk vectors can also help to provide guidance on which aspects of an organization's security processes need improvement.

Rapid changes in the cybersecurity landscape have created a renewed sense among stakeholders of how to reduce the likelihood of business-impacting cybersecurity incidents and strengthen cyber resilience. With the stakes higher than ever, market participants can benefit from analytics that demonstrate which cybersecurity improvements are likely to yield the highest impact. Cybersecurity and cyber risk stakeholders are encouraged to leverage these findings to better serve their respective stakeholders and make more informed and data-backed decisions.

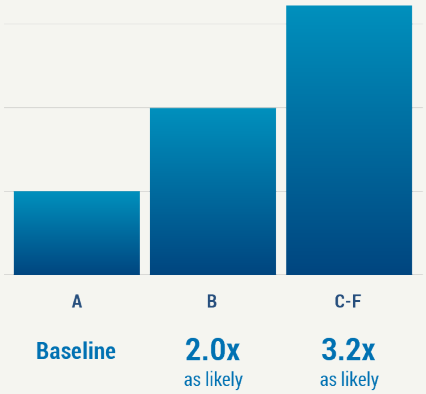
Appendix

The following section includes definitions of the Bitsight risk vectors identified to be closely correlated to cybersecurity incidents and shows the measured value of the relative risk of experiencing a cybersecurity incident as a function of risk vector grade.

Patching Cadence

This Bitsight risk vector measures how many systems within an organization's network are affected by important vulnerabilities and how quickly the organization patches them. Vulnerabilities are publicly disclosed weaknesses or bugs in software that can be used by attackers to gain unauthorized access to systems and data.

Patching Cadence
Cybersecurity incidents vs. an **A-Graded** company



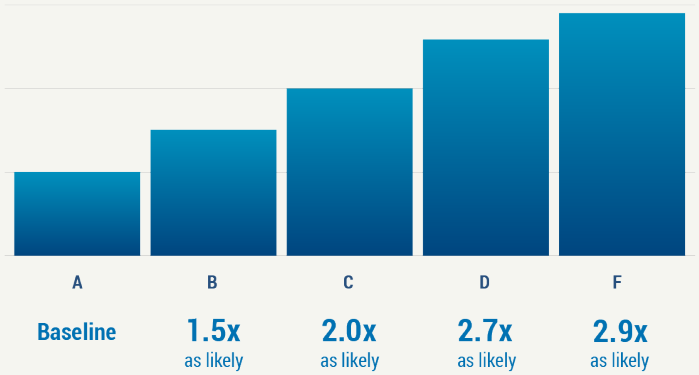
Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

From this analysis, Patching Cadence had the strongest correlation with cybersecurity incidents. However, we note that the relative risk was smaller than Bitsight previously observed when looking solely at ransomware. There may well be a significant difference in correlation between the risk vector grade and the likelihoods of ransomware compared with general cybersecurity incidents for reasons not fully examined in this study.

Desktop Software

This Bitsight risk vector measures whether browsers and operating systems are kept up to date for devices such as laptops, servers, and other non-tablet, non-phone computers in a company's network with access to the Internet.

Desktop Software
Cybersecurity incidents vs. an **A-Graded** company

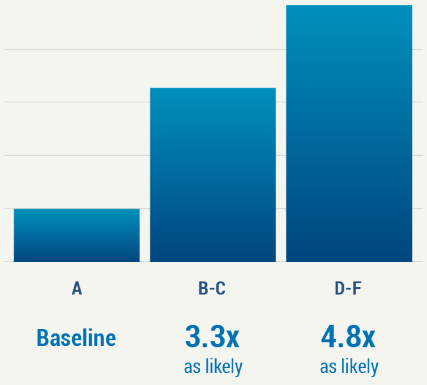


Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

Potentially Exploited

This Bitsight risk vector indicates that a device connected to a company's network is running a potentially unwanted program (PUP) or potentially unwanted application (PUA).

Potentially Exploited
Cybersecurity incidents vs. an **A-Graded** company

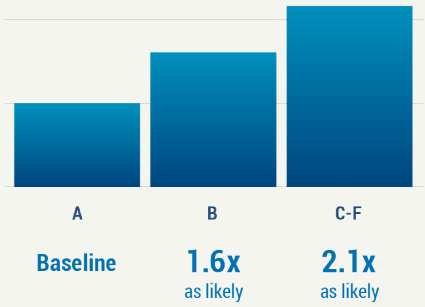


Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

Mobile Software

This Bitsight risk vector measures whether mobile software and associated devices such as phones and tablets are kept up to date.

Mobile Software
Cybersecurity incidents vs. an **A-Graded** company

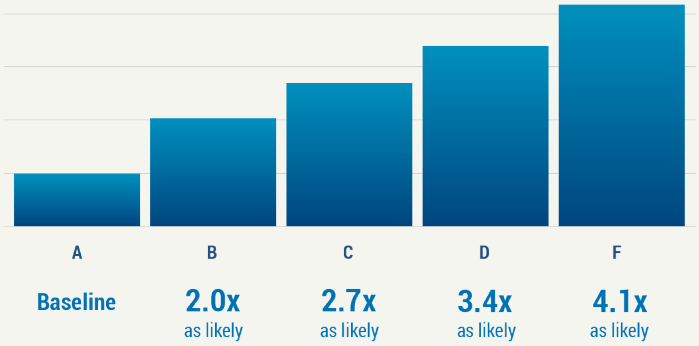


Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

Botnet Infections

This Bitsight risk vector indicates that devices on a company's network are participating in a botnet (combination of "robot" and "network"), either as bots or as a command and control (C&C or C2) server.

Botnet Infections
Cybersecurity incidents vs. an **A-Graded** company

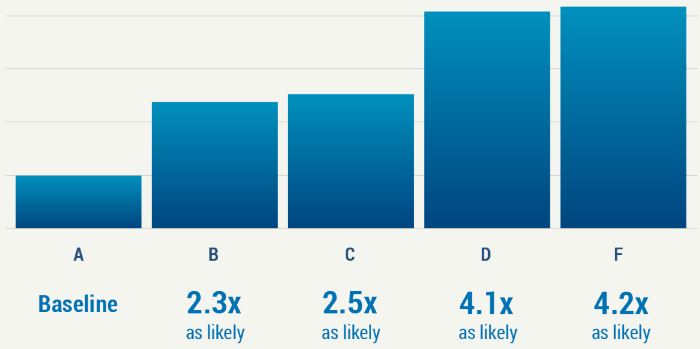


Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

Insecure Systems

This Bitsight risk vector assesses endpoints communicating with an unintended destination. Software on these endpoints may be outdated, tampered with, or misconfigured.

Insecure Systems
Cybersecurity incidents vs. an **A-Graded** company

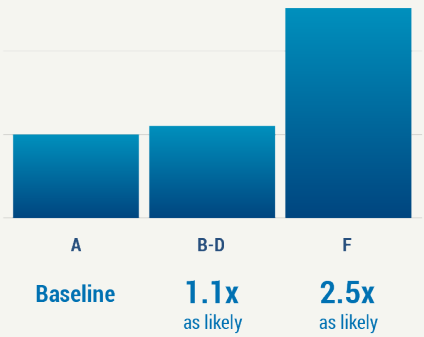


Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

Web Application Headers

This Bitsight risk vector analyzes web server traffic by examining security-related fields in the header section of HTTP request and response messages. If configured correctly, these fields can help protect against malicious behavior, such as man-in-the-middle and cross-site scripting attacks.

Web Application Headers
Cybersecurity incidents vs. an **A-Graded** company

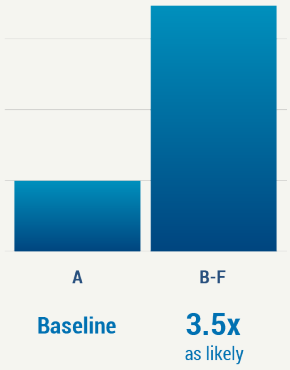


Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

User Behavior

This Bitsight risk vector measures how often employees at an organization are observed engaging in potentially risky behaviors. This includes sharing files using peer-to-peer networks (e.g. BitTorrent). Since these media files and sharing software often come from untrusted sources, they pose a high risk of malware infections.

User Behavior
Cybersecurity incidents vs. an **A-Graded** company

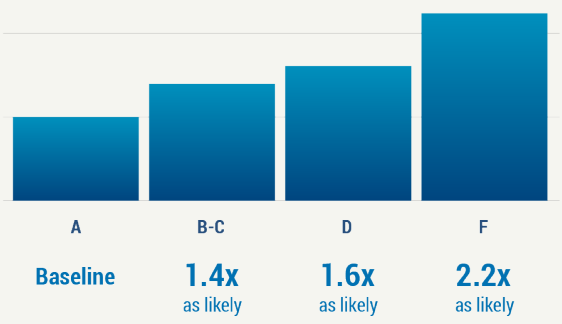


Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

TLS/SSL Configurations

This Bitsight risk vector measures whether a company has correctly configured security encryption software, and whether that software utilizes strong encryption protocols when making encrypted connections to other machines.

TLS/SSL Configurations
Cybersecurity incidents vs. an **A-Graded** company



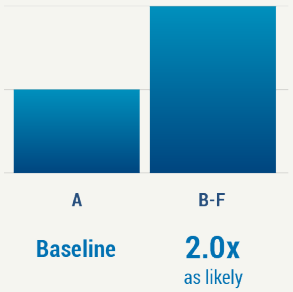
Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

Interestingly, although TLS/SSL Configurations are correlated with ransomware incidents, they do not appear to be as highly correlated with the cybersecurity incidents in Marsh McLennan's proprietary database. It is undetermined at this time whether the reduced correlation of TLS/SSL risk vectors in cybersecurity incidents when compared with ransomware is related to claims payment, policy coverage, or other factors. This will be an area of future research for Bitsight.

Open Ports

This Bitsight risk vector measures 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.

Open Ports
Cybersecurity incidents vs. an **A-Graded** company

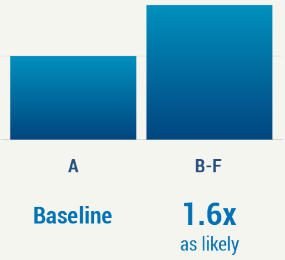


Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

TLS/SSL Certificates

This Bitsight risk vector measures whether the company has properly obtained and deployed TLS/SSL encryption certificates used to secure communication over the Internet. Bitsight analyzes certificates to determine how effective they are at preventing eavesdropping by examining characteristics such as key size and encryption algorithm.

TLS/SSL Certificates
Cybersecurity incidents vs. an **A-Graded** company



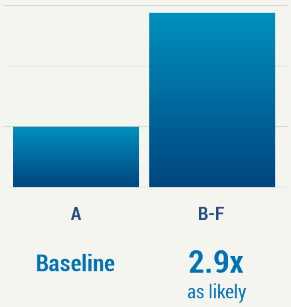
Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

Interestingly, although TLS/SSL Certificates are correlated with ransomware incidents, they do not appear to be as highly correlated with the cybersecurity incidents in Marsh McLennan's proprietary database. It is undetermined at this time whether the reduced correlation of TLS/SSL risk vectors in cybersecurity incidents when compared with ransomware is related to claims payment, policy coverage, or other factors. This will be an area of future research for Bitsight.

Spam Propagation

This Bitsight risk vector measures if an organization is infected with malware and sending unsolicited commercial or bulk email (spam).

Spam Propagation
Cybersecurity incidents vs. an **A-Graded** company

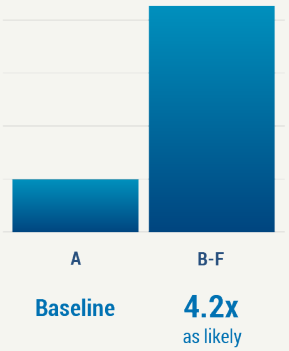


Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

Unsolicited Communications

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

Unsolicited Communications
Cybersecurity incidents vs. an **A-Graded** company

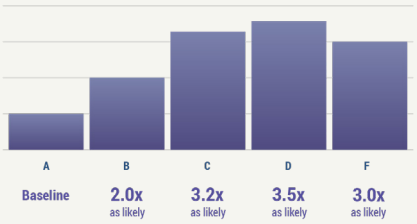


Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

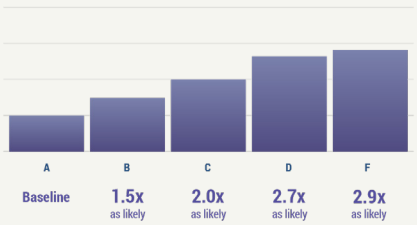
Raw Risk Measurements as a Function of Risk Vector Grade

The charts below show the measured value of the relative risk of experiencing a cybersecurity incident as a function of risk vector grade for the 13 reported Bitsight risk vectors. The values shown below were used to arrive at the grade-combined charts reported earlier in this paper.

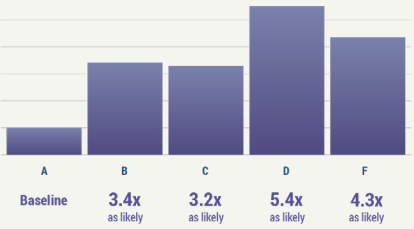
Patching Cadence
Cybersecurity incidents vs. an **A-Graded** company



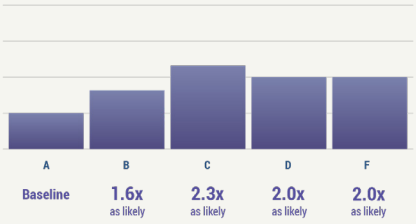
Desktop Software
Cybersecurity incidents vs. an **A-Graded** company



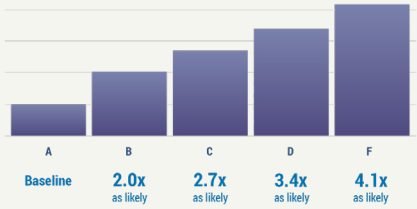
Potentially Exploited
Cybersecurity incidents vs. an **A-Graded** company



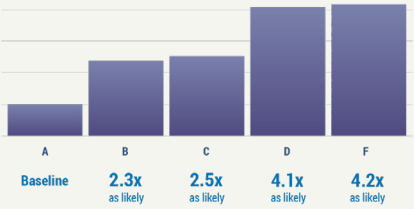
Mobile Software
Cybersecurity incidents vs. an **A-Graded** company



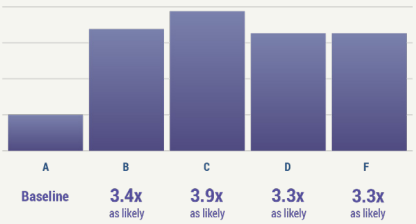
Botnet Infections
Cybersecurity incidents vs. an **A-Graded** company



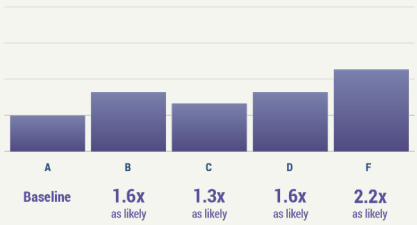
Insecure Systems
Cybersecurity incidents vs. an **A-Graded** company



User Behavior
Cybersecurity incidents vs. an **A-Graded** company

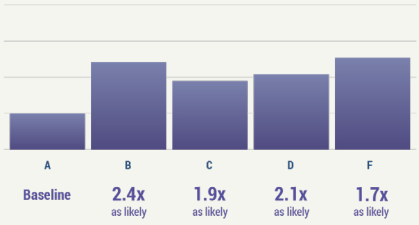


TLS/SSL Configurations
Cybersecurity incidents vs. an **A-Graded** company

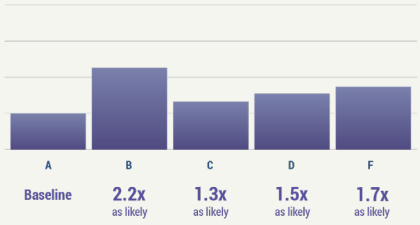


Web Application Headers
Cybersecurity incidents vs. an **A-Graded** company

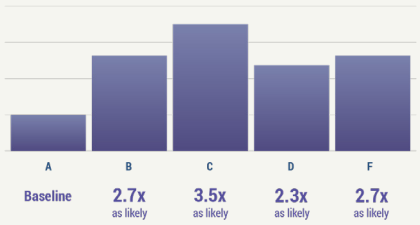
Open Ports
Cybersecurity incidents vs. an **A-Graded** company



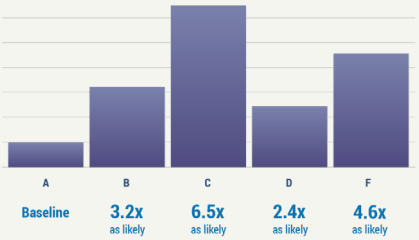
TLS/SSL Certificates
Cybersecurity incidents vs. an **A-Graded** company



Spam Propagation
Cybersecurity incidents vs. an **A-Graded** company



Unsolicited Communications
Cybersecurity incidents vs. an **A-Graded** company



Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

BITSIGHT