BITSIGHT

WHITE PAPER

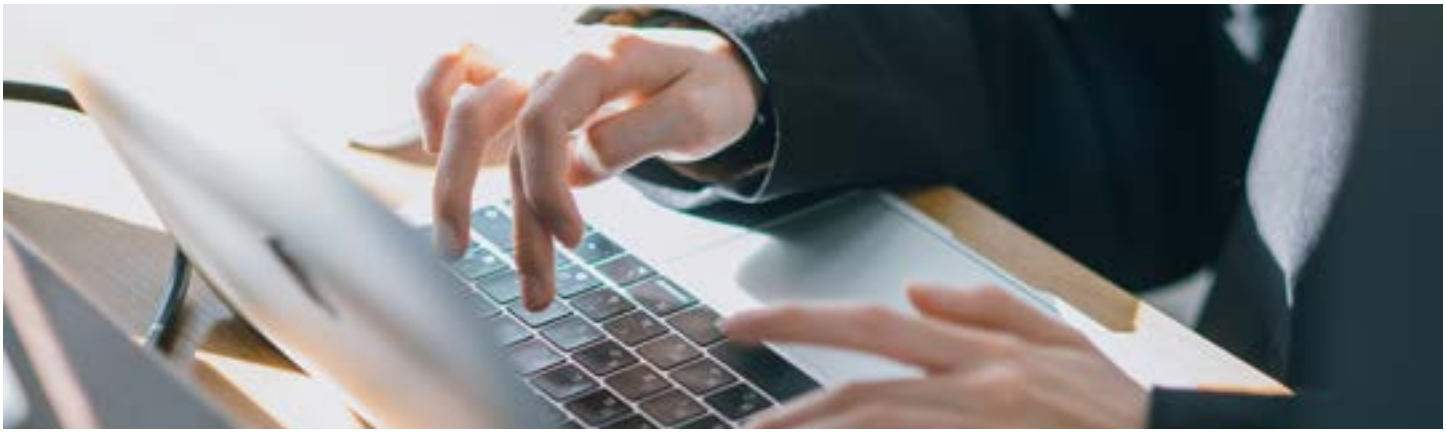
# The Effect of Cyber Management Policies and Program Factors on Cyber Security Performance

Written by John Adams, Joe Lyons

# Introduction

Recent breaches have shown that the operational and reputational impacts can be far-reaching and impactful, reinforcing the idea that cyber risk is business. Now more than ever, it is critical that organizations ensure proper management and governance over their cyber risk programs. Bitsight's leading cyber risk analytics equips business leaders to assess, manage, and quantify cyber risk at scale. In 2021, Moody's Corporation invested $250M into Bitsight, and the two signed a landmark strategic partnership agreement. Through this partnership, Bitsight and Moody's collaborate to bridge the gap between cyber and credit risks.

As part of the effort to bridge the gap between cyber risk and credit risk, Moody's conducted the 2023 Cyber Survey[1]. In June 2023, Moody's surveyed ~2,000 public debt issuers around their respective cyber risk management, transfer, and governance policies – a continuation of its 2021 survey. The '23 Moody's Cyber Survey is now the world's most comprehensive cyber survey regarding respondents' volume and caliber. The derived dataset is a unique lens into the relative cyber risk practices of global corporations, banks, and governments. This paper examines the intersection of this dataset and Bitsight's industry-leading cyber risk analytics. In doing so, a unique view of cyber risk management and best practices was created.



# Analysis & Findings

## Methods

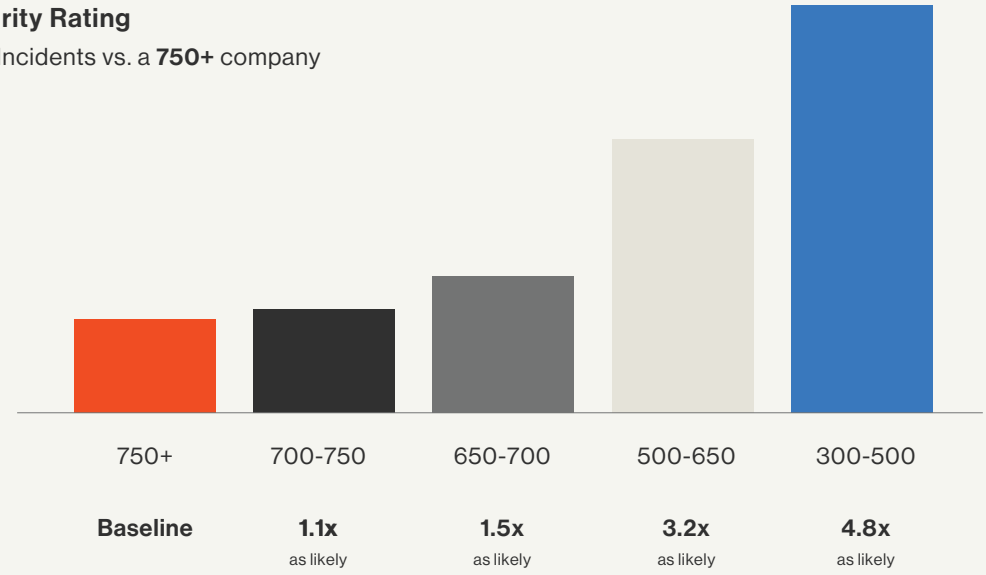
Bitsight analyzed the aggregate statistics of the 2023 Moody's Cyber survey in conjunction with Bitsight security rating data to understand how specific security management policies propagate to security performance at the sector level. We selected the patching cadence Bitsight risk vector (RV) score for examination due to its established correlation to bad outcomes from the 2023 Bitsight/Marsh McLennan study[2]. As a management metric, all "Yes/No" questions from the 2023 Moody's Cyber Survey were analyzed at the sector level. The "Yes/No" questions were translated into a binary measure, where a 'yes' answer indicates the presence of management practices that support a particular aspect of a cyber program (1), and a no assumes that the element of the cyber program is not present (0). Most concisely, this study aims to examine the relationship between a "yes" answer and how its implementation affects an organization's likelihood of cyber incidents.

[1] https://www.moodys.com/web/en/us/about/insights/data-stories/2023-cyber-survey-highlights.html
[2] https://www.bitsight.com/resources/the-marsh-mclennan-cyber-risk-analytics-center-study-finds-statistically-significant-correlation-between-bitsight-analytics-and-cybersecurity-incidents

The following figure shows the measured value of the relative risk of experiencing a cybersecurity incident as a function of the Bitsight Security Rating.

**Bitsight Security Rating**

Cybersecurity Incidents vs. a **750+** company

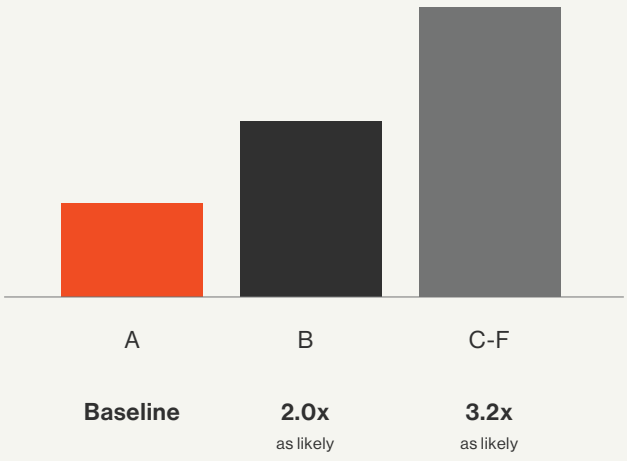



Source: Analysis by Marsh McLennan's Cyber Risk Analytics Center, October 2022

The following figure shows the measured value of the relative risk of experiencing a cybersecurity incident as a function of the patching cadence risk vector. The patching cadence Bitsight risk vector estimates how many systems within an organization's network are affected by high-priority vulnerabilities and how quickly the organization patches them. Vulnerabilities are publicly disclosed weaknesses or bugs in software that attackers can use 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

## Findings

We hypothesized that the absence of specific key cyber program initiatives would adversely affect an organization's cyber performance, increasing its likelihood of experiencing a cyber breach.

Notable Security Ratings findings for "Does the issuer have a vulnerability management program?":

| Question | Score Examined | Sector | Yes Score | No Score | No Risk Increase |
|---|---|---|---|---|---|
| Does the issuer have a vulnerability management program? | Security Rating | Technology | 710 | 655 | 2.0x |
| Does the issuer have a vulnerability management program? | Security Rating | Healthcare Services | 730 | 660 | 2.0x |
| Does the issuer have a vulnerability management program? | Security Rating | Water Services | 700 | 655 | 2.0x |

The above figure shows the difference in the median security rating score for organizations that answered Yes or No to having a vulnerability management program. There is a 2.0x increase in the likelihood of experiencing a cybersecurity incident when an organization in the technology, healthcare, and water services sectors lacks a vulnerability management program.

In conjunction with having poorer overall security, we hypothesized that if a vulnerability management program is absent, we would observe a poor patching cadence grade. The risks of imperfect patching cadence are that these vulnerabilities can expose organizations to malicious attacks. With significant vulnerabilities emerging at an increasing rate, reacting in a timely fashion is critical for reducing cyber risk[3]. Note that an A shows no increase in the risk of experiencing a breach for risk vector grades.

Notable "Patching Cadence findings for Does the issuer have a vulnerability management program?":

| Question | Score Examined | Sector | Yes Score | No Score | No Risk Increase |
|---|---|---|---|---|---|
| Does the issuer have a vulnerability management program? | Patching Cadence | Technology | A | F | 3.2x |
| Does the issuer have a vulnerability management program? | Patching Cadence | Healthcare Services | A | F | 3.2x |
| Does the issuer have a vulnerability management program? | Patching Cadence | Water Services | A | C | 3.2x |

The above figure shows the difference in the median patching cadence risk vector score for organizations that answered Yes or No to having a vulnerability management program. There is a 3.2x increase in the likelihood of experiencing a cybersecurity incident when an organization in the technology, healthcare, and water services sectors lacks a vulnerability management program.

Along with the vulnerability management practices, we hypothesized that a lack of end-of-life software management would lead to poor security performance.

[3] https://help.bitsighttech.com/hc/en-us/articles/231647627-Patching-Cadence-Risk-Vector

Notable Security Rating findings: “Does the issuer have a program to track end-of-life (eol) software?”:

| Question | Score Examined | Sector | Yes Score | No Score | No Risk Increase |
|---|---|---|---|---|---|
| Does the issuer have a program to track end-of-life (eol) software? | Security Rating | Technology | 710 | 680 | 2.0x |
| Does the issuer have a program to track end-of-life (eol) software? | Security Rating | Gaming and Gambling | 650 | 570 | 3.0x |
| Does the issuer have a program to track end-of-life (eol) software? | Security Rating | Consumer Goods | 720 | 680 | 2.0x |

The above figure shows the difference in the median security rating score for organizations that answered Yes or No to having an end-of-life (EOL) program. There is a 3.0x increase in the likelihood of experiencing a cybersecurity incident when an organization in the gaming and gambling sector lacks an end-of-life (EOL) program. There is a 2.0x increase in the likelihood of experiencing a cybersecurity incident when an organization in the Technology and Consumer Goods sectors lacks an end-of-life (EOL) program.

Notable Patching Cadence findings for “Does the issuer have a program to track end-of-life (eol) software?”:

| Question | Score Examined | Sector | Yes Score | No Score | No Risk Increase |
|---|---|---|---|---|---|
| Does the issuer have a program to track end-of-life (eol) software? | Patching Cadence | Technology | B | D | 1.2x |
| Does the issuer have a program to track end-of-life (eol) software? | Patching Cadence | Gaming and Gambling | B | C | 3.2x |
| Does the issuer have a program to track end-of-life (eol) software? | Patching Cadence | Manufacturing | A | C | 1.2x |

The above figure shows the difference in the median patching cadence risk vector score for organizations that answered Yes or No to having an end-of-life (EOL) program. There is a 3.2x increase in the likelihood of experiencing a cyber security incident when an organization in the gaming and gambling sector lacks an end-of-life (EOL) program. There is a 1.2x increase in the likelihood of experiencing a cybersecurity incident when an organization in the Technology and Manufacturing sectors lacks an end-of-life (EOL) program.

# Conclusion

Cyber risk management is transforming how companies manage exposure, performance, and risk for themselves and their third parties. The cross-sectional study of Bitsight's leading cyber risk analytics and Moody's groundbreaking cyber survey dataset allows for new insights into cyber risk management and how security posture is affected. The findings demonstrated that adopting best practices shows sectors and organizations are less likely to experience breach events. The overall Bitsight security rating and patching cadence risk vector scores were highlighted. The security rating is a substantial measure of an organization's overall security posture, and the patching cadence risk vector provides insight into an organization's vulnerabilities and how they are managed. Initial findings show strong correlations between management/program best practices and better cybersecurity posture, particularly in consumer goods, gaming and gambling, healthcare, manufacturing, technology, and water services sectors. The following steps will further this finding and examine the implications of risk posture while having a cyber risk quantification program.

# Moody's & Bitsight

Bitsight is a cyber risk management leader transforming companies' management of exposure, performance, and risk for themselves and their third parties. Moody's is a global integrated risk assessment firm that empowers organizations to make better decisions. Their data, analytical solutions, and insights help decision-makers identify opportunities and manage the risks of doing business with others. With over 14,000 employees in more than 40 countries, Moody's combines global presence with local expertise and over a century of experience in financial markets. In 2021, it was announced that Moody's is investing $250 million in Bitsight to enable organizations to measure their cyber risk accurately.

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