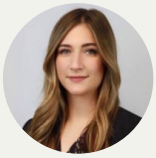
BITSIGHT

WHITE PAPER

Guidance on the Integration of Bitsight Ratings & Data in Investment Analysis

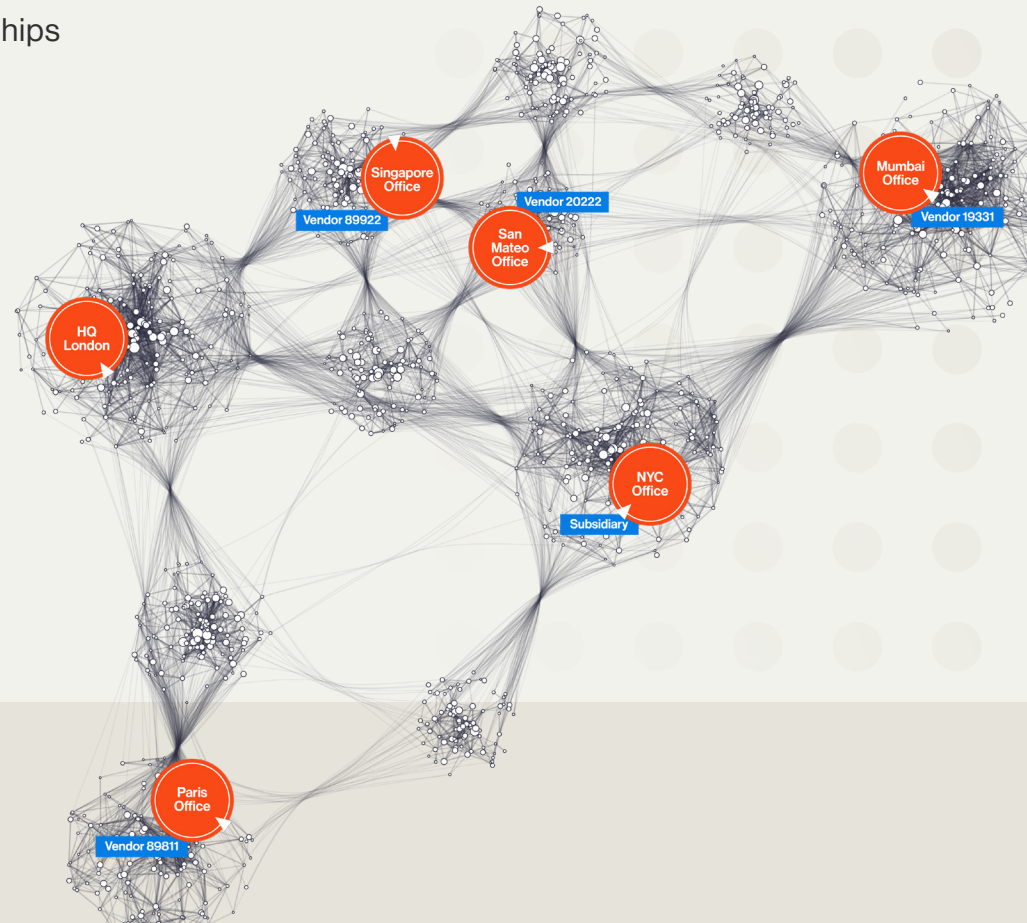
Review of Research, Methodology & Best Practices



Nicole Pastor Matusek
Director, Investment Management Partnerships

Michael Hoffman
VP, Strategic Partnerships

Joe Lyons
VP, Signals &
Ratings Research



Introduction: The Critical Connection between Cybersecurity and Financial Performance and Risk

Growing operational reliance on technology has made cybersecurity both a digital and a physical risk, making it essential to gain visibility into cyber risk exposure across the broader business ecosystem.

The World Economic Forum's 2024 Global Risks Report highlights cyber-related risks as top risks to the global economy that will intensify. Additionally, the report points to growing cyber inequity, a shortage of cyber skills, and predicts the cost of cybercrime could reach $10.5 trillion annually by 2025. Bitsight produces the largest cyber risk ratings and analytics dataset, with daily ratings on up to 40 million entities and the strongest correlation to cybersecurity incidents, including breach and ransomware, as measured by industry leaders such as Marsh McLennan. Bitsight's actionable cyber risk data and analytics with proven correlation to key business outcomes enable investment managers to price and manage cyber risk within their portfolios, enhance their decisioning processes, and mitigate risks effectively to maximize risk-adjusted returns.

Cyber is an unpriced and historically opaque dimension of risk for investors, but continued cyber headlines and regulatory tailwinds are accelerating the awareness and adoption of cybersecurity measures within capital markets, signaling an increasing importance of cyber risk in investment decisions and corporate governance. For instance, the U.S. Securities and Exchange Commission (SEC) introduced new cybersecurity requirements in July 2023, mandating publicly traded companies to disclose "material" cybersecurity incidents within four business days and provide detailed information on their cybersecurity risk management and governance practices. These rules aim to enhance protections for boards, shareholders, and investors by ensuring greater transparency and oversight of corporate cyber risk.

Beyond the SEC, other global regulations reinforce the growing importance of cybersecurity, particularly in the financial sector. In the European Union, the Digital Operational Resilience Act (DORA), adopted in 2022 and set to apply in 2025, mandates financial institutions to manage ICT risks, ensure digital resilience, and report significant cybersecurity incidents to regulators. DORA, alongside established frameworks like GDPR and New York's NYDFS cybersecurity regulation, underscores the global focus on protecting critical financial infrastructures from cyber threats. These regulatory moves, combined with standards like ISO/IEC 27001 and the NIST Cybersecurity Framework, create a comprehensive environment where cybersecurity is a strategic imperative, particularly for organizations managing sensitive data and critical assets.

The World Economic Forum's 2024 Global Risks Report highlights cyber-related risks as top risks to the global economy that will intensify.

Bitsight views these regulatory shifts as key drivers for embedding cybersecurity into capital markets and investment decision-making processes. With increasing obligations for boards and executives to oversee cyber risk, and a clear regulatory expectation for timely cyber incident reporting, market leaders face growing pressure to integrate cyber risk management into their overall corporate strategy. These trends indicate that cybersecurity is no longer just a technical concern but a critical factor influencing corporate governance, risk assessments, and long-term value creation—an essential consideration for asset managers and investors alike.

Investors can leverage Bitsight Security Ratings & Data in a variety of ways:

1. **Enhanced Due Diligence & Underwriting:** Price cyber risk into investment decision making
2. **Alpha Signal:** Identify opportunities for outperformance
3. **Portfolio Risk Management:** Identify high-risk companies to prioritize risk mitigation and engagement activities
4. **Investment Stewardship:** Enhance and protect long-term investment value

The purpose of this paper is to explore the value of Bitsight ratings in investment analysis and to provide methodological guidance and best practices in the integration of cybersecurity ratings in investment analysis. This will include a review of Bitsight's ratings methodology, previous research conducted on Bitsight data and the associated methodologies employed, and other practical considerations for investors.

Bitsight Rating Methodology

Bitsight Security Ratings evaluate the cybersecurity posture of organizations using a comprehensive, data-driven approach. The ratings are based on two types of externally observable data: security events and configuration information. Security events, such as malware distribution, indicate external adversary control, while configuration information checks adherence to cybersecurity best practices. Ratings are calculated daily through a proprietary algorithm that accounts for the number and types of compromised systems, the quantity of outstanding security configuration issues, and the observed duration of these findings.

The ratings are presented on a scale from 250 to 900, with the effective range being 300-820, and categorized into three main levels: Advanced (740-900), Intermediate (640-730), and Basic (250-630). Advanced ratings indicate strong security performance and low risk, Intermediate ratings suggest fair performance and moderate risk, and Basic ratings reflect poor performance and higher risk. These categories help quickly communicate the overall risk posed by an entity, with ratings normalized based on the organization's size for fairness.

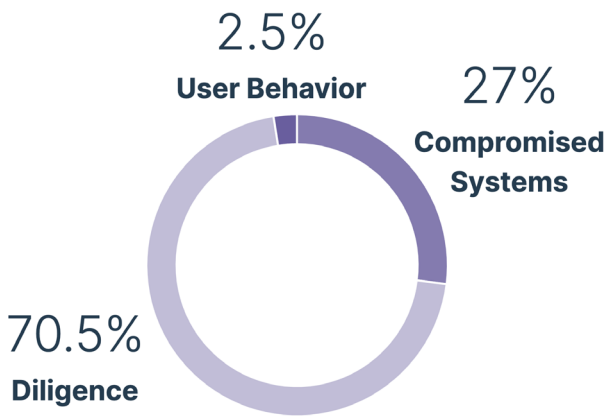
Bitsight's system aggregates data from various risk vectors, such as compromised systems, diligence, user behavior, and public disclosures, with compromised systems and diligence carrying significant weight. Companies receive letter grades from A to F, reflecting their performance relative to peers. This automated service leverages one year of supporting data, providing daily updates and highlighting significant changes.

Bitsight's full rating methodology can be found here.

By analyzing security events and configuration information, Bitsight Security Ratings provide valuable insights into an organization's security performance. Bitsight can also aggregate the ratings of an organization's vendors and partners to help users gain insight into the cyber risk of its supply chain. This innovative, outside-in approach allows organizations to better understand and improve their cybersecurity posture, contributing to enhanced risk management and more informed decision-making. Further, the data Bitsight collects to generate its ratings is externally observable and does not require company disclosure, representing public information for investors and contributing to greater market risk transparency.

Risk Category Weights

Risk categories are weighted as follows (*public disclosures are weighted only if they occur*):



> Bitsight's system aggregates data from various risk vectors, such as compromised systems, diligence, user behavior, and public disclosures, with compromised systems and diligence carrying significant weight.

Review of Research: Methodologies & Results

SOLACTIVE

Solactive Bitsight Cyber Risk Indices →

METHODOLOGY

Solactive uses Bitsight Security Ratings to construct the Solactive Bitsight Cyber Risk Indices. Solactive has developed five distinct indices, four of which are regional:

- Solactive Bitsight Developed Markets Cyber Risk Index
- Solactive Bitsight Europe Cyber Risk Index
- Solactive Bitsight Pacific Cyber Risk Index
- Solactive Bitsight United States Cyber Risk Index
- Solactive Bitsight United States Technology Cyber Risk Index

Solactive selects the top 25% of companies within each sector from their Global Benchmark Series (GBS) Large & Mid Cap Index as the foundation of the indices. This ensures sector neutrality and represents best-in-class companies regarding cybersecurity. The selection criteria for four regional indices are uniform, ensuring a consistent and objective approach across different markets.

The fifth index, focused on the United States technology sector, applies a more detailed methodology. It considers additional risk vector data elements from Bitsight's underlying ratings, providing a nuanced view of cybersecurity performance within this critical sector. The securities in the index are ranked based on their average scores across several Bitsight risk vectors, including SPF Domains, DKIM Records, TLS/SSL Certificates, TLS/SSL Configurations, Open Ports, Web Application Headers, Patching Cadence, Insecure Systems, Server Software, Desktop Software, and Mobile Software. The top 25% of securities, determined by the highest median scores, are selected for inclusion in the index. In cases where securities have the same median score, the one with the higher average daily trading value over the preceding month and six months is ranked higher. General guidance on the use of underlying risk vector data and associated best practices are discussed in more detail in a subsequent section of this paper.

To maintain a balanced representation, all selected companies are equally weighted within the indices. This approach avoids over-concentration in any single entity and ensures that the cybersecurity effectiveness of all included companies is reflected equally. The indices are rebalanced quarterly to account for changes in cybersecurity ratings and market conditions, ensuring the indices remain up-to-date and relevant.

RESULTS

Back-testing of the Solactive Bitsight Cyber Risk Indices demonstrates significant outperformance by companies in the top 25% per sector with the highest Bitsight Security Ratings. In the 5.5 year period from February 2015 to September 2020, the indices generated outperformance ranging from 8.4 to 93.8 percentage points, with the US Technology index achieving the highest at 93.8 percentage points, or approximately 7 percentage points annually. Notably, the regional indices (Developed Markets, Europe, Pacific, and the United States) all generated outperformance over their respective benchmarks as well of approximately 1 to 2 percentage points per year. These findings indicate that companies with superior cybersecurity practices have a competitive advantage and potentially better long-term financial performance. Please reference *Table 1* on the next page for additional details.

TABLE 1: Performance of the Solactive Bitsight Indices, Feb 04, 2015 until Sep 30, 2020

All figures are based on total returns of the indices, in USD. Starting universe is our Solative Global Benchmark Series (GBS), and the benchmark is an equal weight version of the respective GBS Large & Mid Cap Index. (*Please note: The back-test of the US Technology version starts on May 7, 2015, due to data availability.*

USD, TR	DEVELOPED MARKETS		EUROPE		PACIFIC		UNITED STATES		US TECHNOLOGY	
	Bench	CR Index	Bench	CR Index	Bench	CR Index	Bench	CR Index	Bench	CR Index
Total Returns	40.6%	53.7%	24.0%	39.1%	38.7%	48.0%	59.0%	67.4%	152.7%	246.6%
Return p.a.	6.2%	7.9%	3.9%	6.0%	5.9%	7.2%	8.5%	9.5%	18.7%	25.9%
Volatility p.a.	14.1%	13.5%	18.9%	19.1%	15.1%	14.6%	19.1%	19.3%	21.2%	22.1%
Sharpe Ratio	0.44	0.58	0.21	0.31	0.39	0.49	0.45	0.49	0.88	1.17
Drawdown	-36.6%	-35.4%	-38.9%	-38.8%	-33.0%	-31.7%	-38.6%	-39.1%	-33.0%	-33.8%

Diligent

Diligent: Cybersecurity, Audit and the Board: How does board oversight affect cybersecurity performance? →

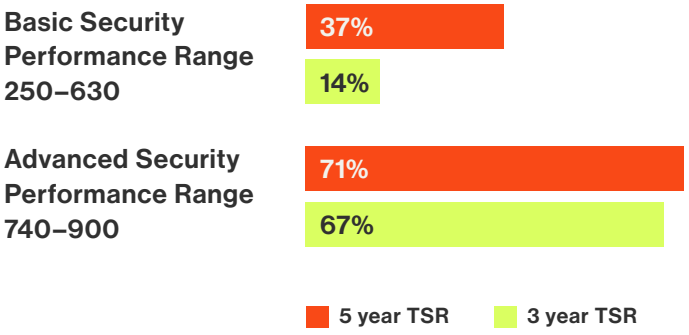
METHODOLOGY

In their analysis, Diligent examined publicly available data on approximately 4,000 mid to large-cap companies across various countries, including Australia, Canada, France, Germany, Japan, the United Kingdom, and the United States. The study, conducted using board data sourced from Diligent Market Intelligence in November 2023, focused on the board structures and director skillsets of these companies. The companies were categorized based on the presence and type of specialized risk committees overseeing cybersecurity, audit committees assuming cybersecurity oversight, or full board oversight in the absence of specific committees. Directors were classified as "cybersecurity experts" if they were current or former CISOs, or had held CEO, CIO, or CTO positions in cybersecurity companies.

The study correlated each company's cyber oversight structure with their Bitsight security performance ratings, collected between December 2023 and February 2024. The research aimed to identify patterns in cybersecurity oversight and performance, providing insights into how board-level governance structures might impact a company's cybersecurity effectiveness.

RESULTS

Diligent's research found that companies with advanced Bitsight ratings generate significantly more value for shareholders compared to those with basic Bitsight ratings. Over a three-year period, the Total Shareholders' Return (TSR) for companies with advanced Bitsight ratings is approximately 372% higher, and over five years, it is 91% higher than that of companies with basic Bitsight ratings. This substantial difference underscores the financial benefits of strong cybersecurity practices. Additionally, companies with specialized risk or audit committees generally exhibit higher security performance, averaging a Bitsight rating of 710 compared to 650 for companies without such committees. The presence of these committees often correlates with a distribution of Bitsight ratings skewing towards the advanced security performance range.



Furthermore, the integration of cybersecurity experts into board committees responsible for cybersecurity oversight significantly enhances an organization's security performance. Simply having a cybersecurity expert on the board does not necessarily lead to higher security ratings. Companies with experts on either audit committees or specialized risk committees have an average security rating of 700, while those without experts in these roles have an average rating of 580. Despite the clear benefits, only 5% of companies have cybersecurity experts on their boards. Additionally, highly regulated industries, such as financial services and healthcare, tend to have better cybersecurity performance, with average ratings of 720 and 730, respectively. In contrast, sectors like industrials and communications have lower average ratings, with the latter scoring the lowest at 630.

MOODY'S

Moody's Ratings: The impact of cybersecurity management practices on the likelihood of cyber events and its effect on financial risk →

METHODOLOGY

The study aimed to estimate expected losses from cyber events by examining the probability of such events occurring and the financial impact they entail. The methodology involved two main components: a logistic model for estimating the probability of cyber incidents and an event study approach to assess financial consequences.

A logistic (logit) model was used to predict the likelihood of a cyber event based on firm characteristics, including industry, size, and cybersecurity performance, as indicated by Bitsight Ratings. The model transformed these variables into probabilities, helping organizations assess and manage cyber risks.

An event study methodology was employed to measure the impact of cyber incidents on company stock prices. This involves calculating abnormal returns, which are the differences between expected and observed equity returns following a cyber event. The study used a market model to estimate expected returns, with a focus on deviations caused by cyber incidents.

Bitsight Ratings were used to evaluate companies' security performance. The analysis considered the severity of cyber events, classified into levels from informational to severe. The integration of Bitsight Ratings into the logistic model enables quantification of the probability of cyber events, while the event study approach provided a framework to understand their financial implications, including impacts on credit risk and equity value. The data spanned from January 2015 to March 2023, offering a robust basis for understanding trends and the long-term effects of cybersecurity practices.

RESULTS

The analysis revealed that the probability of a cyber incident is significantly influenced by a company's cybersecurity practices, industry, and size. Companies with lower Bitsight Ratings are more vulnerable to cyber-attacks, with larger firms facing increased risks due to their expansive workforce and complex IT systems. This heightened vulnerability is reflected in the statistically significant negative abnormal equity returns observed over a 12-month period following a cyber incident. Specifically, the study found that the average stock price declines by 0.54% to 5.352%, depending on the severity of the cyber event, with more severe incidents leading to larger and longer-lasting negative returns. Additionally, the probability of a cyber incident correlates strongly with the company's cybersecurity performance and size, indicating that improved cybersecurity measures can reduce the likelihood of attacks.

The financial impact of cyber incidents also extends to credit risk. The research shows that equity value declines linked to cyber events can increase the probability of default, with a 0.18% rise in default probability observed one month post-incident and a 0.24% increase after twelve months. The effect varies across industries, with Finance, Healthcare, and Technology sectors displaying resilience against financial losses despite frequent attacks. Conversely, sectors such as Real Estate, Tourism, and Media experience higher average losses, highlighting the need for tailored cybersecurity measures. These findings underscore the critical importance of integrating robust cybersecurity practices into broader risk management strategies to safeguard financial stability and mitigate potential credit risks.

MarshMcLennan

Marsh McLennan: Quantifying relationships between cybersecurity performance and likelihood of cybersecurity incidents →

METHODOLOGY

Bitsight provided Marsh McLennan with a comprehensive cybersecurity performance data set, including Security Ratings and risk vectors for 365,000 organizations. Marsh McLennan's Cyber Risk Analytics Center analyzed this data to determine the correlation between Bitsight's cyber risk analytics and the likelihood of cybersecurity incidents. The study also incorporated Marsh McLennan's proprietary data on cyber claims and incidents from 2018 to 2021. They identified 14 analytics, including the Bitsight Security Rating and 13 risk vectors, that showed significant correlation with reported cybersecurity incidents.

To evaluate the correlation, Marsh McLennan matched companies from the Bitsight data to those with cyber insurance policies. They analyzed nearly 16,000 company-years of incident data, finding a 2.35% incident rate. By comparing annual incident data with Bitsight's Security Ratings and risk vector scores, Marsh McLennan estimated the predictive power of these analytics using Rank-Biserial Correlation Coefficients. This method, which ranges from 1 (perfect correlation) to -1 (perfect anti-correlation), indicated that lower performance ratings were linked to higher incident risk. They provided both the correlation statistics and relative risk interpretations to better understand the impact of Bitsight's analytics on predicting cybersecurity incidents.

RESULTS

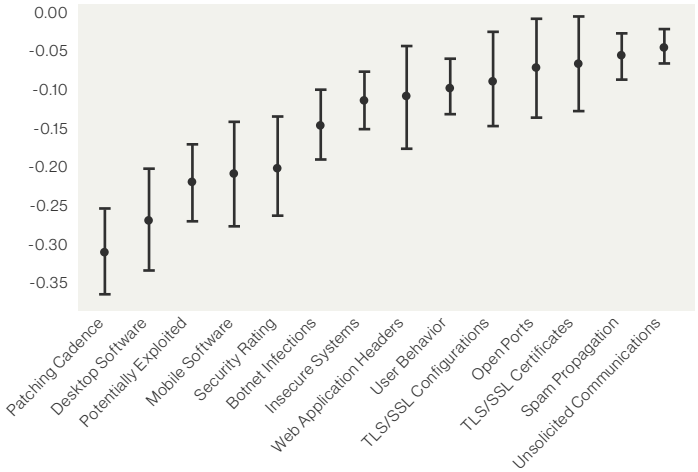
Marsh McLennan's analysis revealed statistically significant correlations between Bitsight analytics and cybersecurity incidents. The study estimated the Rank-Biserial Correlation for Bitsight's Security Rating and risk vectors, finding 14 significant correlations, including the overall Security Rating and 13 risk vectors.

The most correlated risk vectors with cybersecurity incidents were Patching Cadence, Desktop Software, Potentially Exploited, and Mobile Software, aligning with previous Bitsight research. The Security Rating ranked fifth, influenced by the weight of its highly correlated components. Bitsight plans to update its rating algorithm based on these findings.

The analysis showed a significant increase in cybersecurity incident risk as the overall Security Rating dropped below 700. Relative risk estimates highlighted that companies with ratings between 500-650 and 300-500 were 3.2 and 4.8 times more likely to experience incidents, respectively, compared to those rated 750+.

Further analysis demonstrated clear correlations between poor performance in specific risk vectors and increased incident risk, particularly in Endpoint Management, Malware Detection, and Vulnerability Management, with relative risk peaking between 2 and 5 times higher. Statistical uncertainties were noted in some fluctuating risk estimates for lower grades.

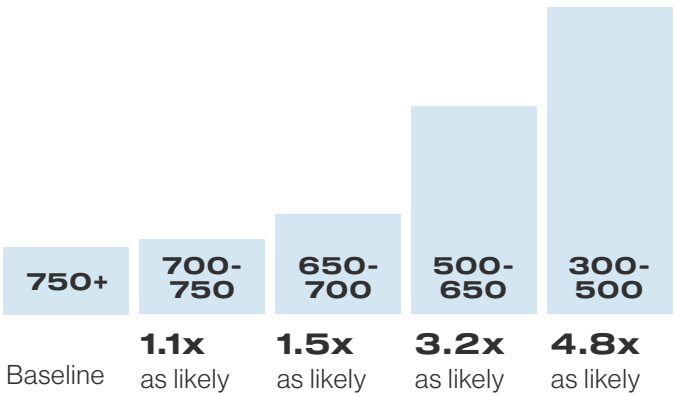
Rank-Biserial Correlation



Bitsight analytics

Bitsight Security Rating

Cybersecurity incidents vs. a 750+ company



Bitsight Guidance on Approaches to Identifying Signal

Application of Marsh McLennan — Risk Vector Analysis

The Marsh McLennan Cyber Risk Analytics Center study, discussed in the previous section of this paper, found that Bitsight's Security Rating and 13 risk vectors were statistically significant in predicting cybersecurity incidents. Lower security ratings (below 700) were strongly correlated with increased incident risk. For investors, focusing on companies with strong performance in certain risk vectors can signal a lower likelihood of incidents. The study highlighted **Patching Cadence, Desktop Software, Mobile Software, Insecure Systems, Potentially Exploited Systems**, and **Botnet Infections** as the most predictive of incidents, making these critical to evaluate.

For investors, the most valuable methods to apply this research are outlier identification and peer group analysis to enhance investment risk decision making.

To leverage the Marsh McLennan study for outlier identification, begin by ranking portfolio companies from weakest to strongest based on the sum of six critical cyber risk vectors. Companies with a "D" or "F" in any of these vectors should be flagged for increased scrutiny.

Performing peer group analysis allows you to benchmark a company's cyber risk performance against its industry counterparts. To conduct peer group analysis, compare the company's cyber risk score with others in the same sector, focusing on the six key vectors, especially patching cadence and desktop software. Assess where the company lags behind peers and prioritize discussions on these weaknesses in upcoming management meetings. This benchmarking ensures that portfolio companies are not only held to absolute cybersecurity standards but also relative ones, providing a comprehensive view of their competitive positioning in managing cyber risks.

Practical applications in quantitative analysis include, but are not limited to, the following:

MINIMUM GRADES:

Dummy Variable for Minimum Grade: Create a dummy variable that indicates whether the minimum grade among the 13 risk vectors is a "D" or "F" (1 if any risk factor is an "F", 0 otherwise). This variable can help assess if having at least one"D" or "F" is statistically significant in its correlation with returns.

Ordinal Representation of Risk Vectors: Treat the minimum grade as an ordinal variable (e.g., A=1, B=2, ..., F=6). This approach assumes a graded scale of risk, with higher values indicating worse performance.

NUMBER OF "D" OR "F" GRADES:

Count Variable: Use the count of "D" or "F" grades as a continuous predictor. This variable captures the extent of negative data across the 13 risk factors. A higher count of "D" or "F" grades would indicate a higher overall risk.

Threshold Variables: Create multiple dummy variables for different thresholds of "D" or "F" grades (e.g., 1 if the number of "D"s "F"s is greater than 5, 0 otherwise). This can help identify specific tipping points where the risk significantly increases.

Incorporate these insights into your investment process, using this information to adjust position sizes, engage in stewardship activities, or make reallocation decisions. Screen companies during due diligence for new investments by evaluating their performance across these key vectors. Companies with weak performance in any of these areas should be assigned higher risk scores. Monitor companies within the portfolio and adjust their risk scores as cybersecurity practices evolve. Improvements in vectors such as patching cadence or desktop software management should result in lower risk scores, while a decline in performance should trigger upward adjustments. Engage with company management to inform them of their cyber risk weaknesses and inquire about remediation efforts.

Regular assessments facilitate proactive risk management, allowing investors to allocate resources to areas most in need of improvement while reducing exposure to companies that show no progress. Cyber risk can impact a company's creditworthiness, influencing bond pricing or default risk. Applying these risk vectors during analysis can help identify companies at greater risk of cyber incidents, particularly those with poor patching cadence or botnet infections. This analysis can guide decisions related to asset allocation, pricing, or retention based on the associated credit risk. For equity investors, incorporating cyber risk factors allows for adjustments in position sizes and enables the evaluation of potential disruptions to earnings resulting from cyber incidents.

By incorporating these high-correlation risk vectors into a structured risk model, investors can more accurately quantify and manage cybersecurity risk across their portfolios. This proactive approach allows for more informed decision-making, targeted risk mitigation efforts, and ultimately stronger resilience against cyber threats across the investment landscape.

Case Studies / Application

The applicability of cyber risk data to capital markets decision-making is expanding rapidly, with diverse use cases emerging across the sector. Here, we explore notable applications of Bitsight's cyber data to date.

Nomura Asset Management

Recognizing the substantial implications of cyber risk on business performance, Nomura Asset Management (NAM) sought to proactively mitigate these risks within its credit portfolios. In collaboration with Bitsight, NAM implemented a comprehensive framework to assess and manage cyber risk, enhancing portfolio resilience and optimizing risk-adjusted returns. Utilizing Bitsight's advanced analytics and structured workflows, NAM was able to systematically engage with portfolio companies, incorporating cybersecurity as a critical component of corporate governance and risk management.

The collaboration focused on the multinational development bank (MNDB) sector, where NAM leveraged Bitsight's capabilities to evaluate the cybersecurity management practices of issuers. The analysis revealed a general trend of intermediate-to-advanced cybersecurity performance across the sector. However, certain issuers demonstrated high-risk ratings that correlated with increased ransomware incident risks. NAM engaged these high-risk issuers through targeted discussions, integrating cybersecurity into their governance frameworks and establishing dialogue with Chief Information Security Officers (CISOs). This engagement resulted in the implementation of new cybersecurity policies and risk mitigation measures by one of the identified high-risk issuers.

Within a three-month period, NAM independently confirmed a quantifiable improvement in the issuer's cybersecurity practices through the Bitsight platform, including significant reductions in associated cyber incident risks. This case illustrates the effectiveness of employing real-time cybersecurity performance data and analytics in guiding investor engagement and decision-making. By integrating cyber risk into their investment processes, NAM was able to foster measurable improvements in the cybersecurity posture of their portfolio companies. The partnership between NAM and Bitsight demonstrates the strategic value of incorporating cybersecurity analytics into portfolio management to enhance risk governance and support sustainable financial performance.

NOMURA

Within a three-month period, NAM independently confirmed a quantifiable improvement in the issuer's cybersecurity practices through the Bitsight platform, including significant reductions in associated cyber incident risks.

MOODY'S

Bitsight detected poor performance before the breach occurred, indicating higher risk of an incident.

Moody's Ratings Credit Negative Comments Due to Cyber Breach

Since 2014, Moody's Ratings has taken 23 credit ratings actions related to cyber risk, highlighting an increasingly critical intersection between cybersecurity performance and credit quality. These actions underscore the significant risks that cyber incidents can pose to an organization's financial stability and reputation. Moody's Ratings has also published many credit negative comments following a breach disclosure. In each of the following examples, Bitsight detected poor performance before the breach occurred, indicating higher risk of an incident.

1 Clorox

On August 14, 2024, Clorox disclosed unusual activity on its IT systems through an 8-K filing, marking the beginning of a significant cyber incident. By August 17, the company activated its business continuity plans, which included reverting to manual processes for handling orders and communicating with customers. Despite these efforts, disruptions persisted. On September 5, Clorox implemented an interim solution that allowed for manual order processing and shipping to resume. The company also resumed production and maintained constant communication with customers to manage immediate concerns.

However, by September 18, the operational disruptions continued, forcing Clorox to scale back its order processing capabilities, leading to reduced product availability in retail outlets. On September 29, Clorox reported that all manufacturing sites were operational again and that the company had started transitioning back to automated order processing. Nevertheless, the company acknowledged that the incident had materially impacted its first-quarter financial results, signaling long-term consequences.

CLOROX

By October 4, Clorox announced it expected a loss for the quarter, a stark contrast to the nearly $150 million in profit that investors had anticipated. The company projected a 23% to 28% decrease in Q1 2024 net sales compared to the previous year. On October 5, The Wall Street Journal reported that Clorox had already spent $25 million in costs directly related to the cyberattack, with additional expenses expected through March. Finally, on October 6, Moody's Ratings published a comment labeling the incident a credit negative event, highlighting the impact of the cyberattack on Q1 earnings and noting that while the disruptions would affect future quarters, the impact would diminish over time.

The Wall Street Journal reported that Clorox had already spent $25 million in costs directly related to the cyberattack, with additional expenses expected through March.[1]

[1] *https://www.wsj.com/articles/clorox-warns-of-accruing-costs-from-cyberattack-a0bc5b6a*

2 Caesars Entertainment

On August 18, a social-engineering attack targeted an outsourced IT support vendor, enabling unauthorized access to users' credentials. Following this, a data breach was discovered on September 7, which had occurred on August 23. On September 14, an 8-K disclosure revealed details of the cyberattack from September 7, indicating that the unauthorized actor had acquired various data, including a loyalty program database containing driver's license numbers and social security numbers for a significant number of members. Additionally, the Wall Street Journal reported on the same day that Caesars had paid approximately half of a $30 million ransom demanded by the hackers.[2] Moody's Ratings also issued a statement that day, declaring the cyberattack credit negative, although it would not impact the company's ratings or outlook. Lastly, on September 18, IT service management company Okta confirmed that five of its clients, including MGM and Caesars Entertainment, had been targeted by the hacking groups ALPHV and Scattered Spider since August.

IT service management company Okta confirmed that five of its clients, including MGM and Caesars Entertainment, had been targeted by the hacking groups ALPHV and Scattered Spider since August.

[2] *https://www.wsj.com/business/hospitality/caesars-paid-ransom-after-suffering-cyberattack-7792c7f0*

3 Change Healthcare

On February 21, 2024, Change Healthcare experienced a cybersecurity breach, prompting the company to isolate its systems to prevent further damage. Two days later, on February 23, Moody's Ratings deemed the incident credit negative, highlighting the potential financial repercussions. By March 4, the American Hospital Association (AHA) criticized Change Healthcare's funding program as inadequate, as some healthcare providers began losing more than $100 million daily due to the disruption.

On March 6, UnitedHealth Group, which owns Change Healthcare, faced five federal lawsuits related to the attack, according to HealthLeaders Media.[3] A week later, on March 13, UnitedHealth announced that Change Healthcare's pharmacy network was back online, marking a step toward recovery. However, the financial toll became clearer on April 22, when UnitedHealth revealed that the ransomware attack had cost $872 million in the first quarter alone. According to UnitedHealth Group's 2024 year-end earnings report, the total impact of the cyberattack at its Change Healthcare unit was $3.09 billion, including $2.2 billion in direct response costs and $867 million in business disruption. In response to the crisis, Change Healthcare funneled $9 billion in advance funding and loans to support affected healthcare providers, though full recovery from the cyberattack had not yet been achieved.

On May 3, new details emerged during UnitedHealth Group CEO Andrew Witty's testimony before the U.S. House Energy and Commerce Committee. Witty disclosed that cyber operatives had used stolen credentials to access a remote access tool that was not secured with multifactor authentication (MFA), allowing them to breach UnitedHealth's network. The ransomware group AlphV/BlackCat was identified as the attacker, hijacking Change Healthcare's systems and demanding a ransom to unlock them.

[2] *https://www.healthleadersmedia.com/technology/timeline-change-healthcare-attack*

4 MGM Resorts

On September 11, MGM Resorts issued a press release announcing that a "cybersecurity incident" had affected some of its systems, prompting an investigation into the attack and the involvement of relevant authorities. The following day, on September 12, MGM filed an 8-K disclosure detailing the press release issued regarding the cybersecurity issue. Simultaneously, guests began reporting problems with the company's online booking system and casino, and MGM's main website was also reported as down.

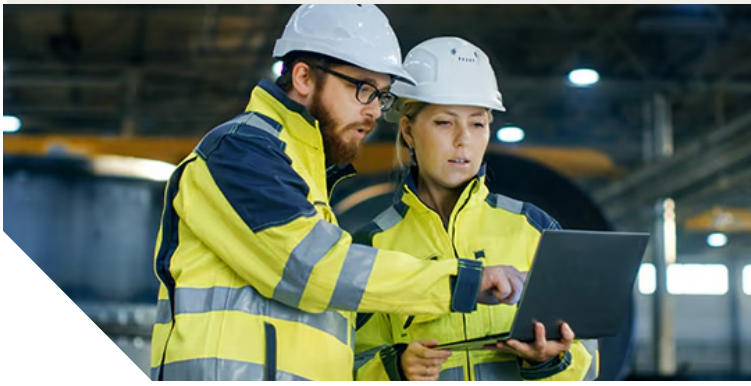
By September 13, Moody's Ratings published an issuer comment stating that the incident was credit negative for MGM, emphasizing the risks posed by the company's reliance on technology and the significant operational disruptions that occur when systems are taken offline. On September 18, Okta, an IT service management company, confirmed that hacking groups ALPHV and Scattered Spider had targeted five of its clients, including MGM Resorts and Caesars Entertainment, since August.

> MGM revealed the full extent of the damage, announcing that the cyberattack had cost the company $100 million in lost earnings.

MGM Resorts' computer systems were finally restored after a 10-day outage on September 21. However, on October 5, MGM revealed the full extent of the damage, announcing that the cyberattack had cost the company $100 million in lost earnings. Additionally, the attack compromised customers' personal information. MGM also incurred less than $10 million in one-time expenses related to risk remediation, legal fees, third-party advisory services, and incident response measures. Despite these losses, MGM stated that it expects full coverage under its cybersecurity insurance.

5 Johnson Controls International

On September 27, Johnson Controls International (JCI) filed an 8-K disclosure regarding disruptions in parts of its internal information technology infrastructure and applications due to a cybersecurity incident. On the same day, it was reported that the company suffered a massive ransomware attack, demanding a ransom of $51 million, which resulted in the encryption of numerous devices and significantly impacted the operations of both JCI and its subsidiaries. Following this, on September 28, JCI's stock fell as much as 5.7%, marking its largest decline in two months, in response to the announcement of the "cybersecurity incident" that had disrupted its computer networks. The following day, Moody's Ratings issued a comment noting that the incident is credit negative for the company, emphasizing the risks associated with an increasing reliance on technology for business operations and the disruptions that occur when digital systems are compromised. As of now, the root cause of the incident remains unknown. On October 2, senior officials from the Department of Homeland Security began investigating whether the ransomware attack on JCI had compromised sensitive physical security information, such as DHS floor plans, as indicated in internal DHS correspondence reviewed by CNN.



On October 28, 2023, Mueller identified a cybersecurity incident resulting in delays in various business operations that could negatively affect the company's financial results.

6 Mueller Water Products

On October 28, 2023, Mueller Water Products, Inc. identified a cybersecurity incident that impacted certain operational and information technology systems, resulting in delays in various business operations that could negatively affect the company's financial results. By November 29, 2024, Mueller Water Products reported that all facilities had substantially returned to normal operations following the incident. However, the company indicated that it would delay its 10-K filing due to the disruptions caused by the incident, which affected access to certain systems and information. On January 3, 2024, Moody's Ratings released a report on Mueller Water Products, stating that the cybersecurity incident was credit negative for the company.

7 Ivanti Software, Inc.

On January 11, 2024, a pair of zero-day vulnerabilities were identified in Ivanti Connect Secure (ICS) and Policy Secure, which were reportedly exploited by suspected China-linked nation-state actors to breach fewer than ten customers. By January 16, Ivanti acknowledged a surge in hacking attempts targeting these recently disclosed vulnerabilities in its Connect Secure VPN product, with cybersecurity researchers estimating that approximately 1,700 devices had been compromised worldwide. On January 19, the Cybersecurity and Infrastructure Security Agency (CISA) ordered civilian agencies across the U.S. government to immediately patch the vulnerabilities in Ivanti's popular tools, following warnings of widespread exploitation of CVE-2023-46805 and CVE-2024-21887. On the same day, Moody's Ratings reported that the two zero-day vulnerabilities in the VPN were credit negative for Ivanti.

8 AT&T

Between April 14 and 25, 2024, a significant data breach occurred in which call logs from AT&T were stolen, impacting approximately 7.6 million current customers and 65.4 million former account holders. On April 19, 2024, AT&T acknowledged that it had become aware of hackers claiming responsibility for stealing the data. On May 17, 2024, a hacker associated with the ShinyHunters group claimed that AT&T made a ransom payment of $373,646 to address the breach.

On June 5, 2024, the U.S. Department of Justice stated that there was a justified delay in the public disclosure of the breach. It wasn't until July 12, 2024, that AT&T issued a public press release to inform the public about the incident. "This latest announced AT&T breach is a credit negative that raises serious questions about the company's cyber risk governance and management practices," Moody's Ratings Vice President – Senior Analyst Neil Mack said in an emailed statement. "A key risk is of customer defections as a result of customers' perceiving their private data being more vulnerable at AT&T relative to wireless competitors."

Cyber and Broader Technological Resilience

CROWDSTRIKE INCIDENT

The recent CrowdStrike incident exemplifies significant operational risk stemming from an internal technical failure. The incident involved a critical misconfiguration during a routine update within CrowdStrike's data centers, which resulted in a temporary outage of its Falcon platform. This platform is essential for delivering real-time threat detection and response services to a global clientele. Consequently, the outage disrupted operations, affecting numerous customers reliant on uninterrupted access to cybersecurity solutions. Although this event did not involve a malicious cyberattack, it serves to underscore the potential vulnerabilities that even the most sophisticated firms can encounter due to internal technological failures.

This occurrence highlights the importance of technological oversight—the effective management and governance of internal systems and processes to mitigate the risk of service interruptions. The operational impact of the CrowdStrike incident demonstrates the necessity for operational resilience within organizations, particularly in an interconnected digital ecosystem where disruptions can reverberate through supply chains and affect stakeholders significantly.

Furthermore, the incident emphasizes the value of utilizing Bitsight's cybersecurity ratings and other performance metrics as tools for assessing not only a company's cyber risk but also its overall technology management capabilities. A company's cybersecurity rating can provide insights into its capacity to manage both cyber threats and its broader digital infrastructure. In this context, technological vulnerabilities such as those experienced by CrowdStrike serve as indicators of potential deficiencies in organizational governance. Thus, understanding digital risks in a comprehensive manner is critical for ensuring resilience in the contemporary interconnected economy. This incident illustrates the imperative for organizations to prioritize robust technological oversight and operational resilience as integral components of their strategic risk management frameworks.

Use of Bitsight Data in New Analytics

IMPLIED CYBER THREAT

Bitsight's Implied Cyber Threat analytic is a firmographic-based tool designed to assess the inherent cybersecurity risks of over 400 million organizations globally. It incorporates firmographic factors such as company size, sector, and geographic location, along with technographic data like botnet infections, potentially exploited systems, and open ports. This information is used to categorize organizations into five risk levels—Very Low to Very High—allowing risk managers to evaluate the likelihood of cybersecurity incidents impacting business operations.

The analytic is particularly valuable for risk practitioners who are not cybersecurity experts but need to incorporate cyber risk into broader risk management processes, such as mergers and acquisitions, supplier management, and financial assessments. It offers a scalable and comparable measure of cyber risk that can be used independently or alongside Bitsight's existing security ratings. The model is continuously updated and validated with real-world data, providing actionable insights for making informed business decisions in a dynamic cybersecurity landscape.

Bitsight's Implied Cyber Threat analytic is a firmographic-based tool designed to assess the inherent cybersecurity risks of over 400 million organizations globally.

Conclusion

The integration of cybersecurity ratings into investment decision making is no longer optional but an imperative. As cyber threats continue to evolve and intensify, the financial and operational impacts on companies—and by extension, their investors—are becoming clearer. Leveraging Bitsight's robust dataset and analytics, investment decision makers can achieve a deeper understanding of cyber risks, enabling them to identify opportunities for outperformance, mitigate potential portfolio risks, and enhance risk-adjusted returns

Through demonstrated methodologies and case studies, this paper highlights how Bitsight ratings can act as a predictive tool for financial resilience, guiding due diligence, portfolio management, and engagement strategies. From back-tested index outperformance to Moody's Ratings credit implications for cyber breaches, the evidence underscores the importance of cybersecurity in financial outcomes. Moreover, granular risk vector analysis offers actionable insights to pinpoint vulnerabilities and prioritize engagement with portfolio companies.

Incorporating these tools into investment strategies can empower asset managers to navigate a rapidly shifting risk landscape with greater precision and confidence. By embedding cybersecurity considerations into investment frameworks, investors not only safeguard their portfolios but also drive corporate accountability and resilience. As regulatory environments tighten and the stakes of cyber incidents rise, proactive use of cybersecurity data will distinguish forward-thinking investors, positioning them for sustainable success in the digital economy.

This paradigm shift transforms cybersecurity from a technical consideration into a core driver of financial and strategic decision-making. Investment leaders who embrace these insights stand to not only protect their capital but also uncover hidden opportunities for growth and innovation in an increasingly digitally interconnected world.

Take the Next Step

If you're interested in exploring how Bitsight ratings and data can enhance your investment strategies or if you have questions about the guidance provided in this paper, we encourage you to reach out. Our team is here to support you in leveraging this innovative data to gain deeper insights and make more informed decisions.

Contact us today.

Bitsight Investor Business Team
investorbusiness@bitsight.com

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

BITSIGHT