MOODY'S

Cyber security and its effects on financial risk

Alejandra Caro Rincon
Associate Director, Predictive Analytics

Introduction

Channels for cyber to impact credit impact

→ Cyber risk is an operational risk that can have knock on effects on other risks.

→ Assessing the impact of a cyber event is challenging as it doesn't always result in immediate material consequences.

→ Additional factors with indirect financial implications are crucial in assessing how a cybersecurity event can directly affect credit standing.

Business Disruption

Operational disruption can last for days/weeks and have a negative impact on revenue generation and expenses

Fraud

Diverting payments such as interest payments can trigger events of defaults under loan agreements

Regulatory + Reputational Risk

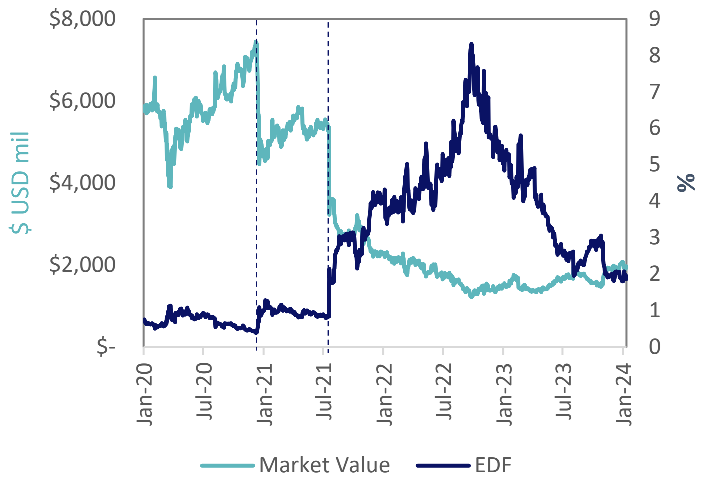
Inadequate cyber risk mitigation practices can trigger increased regulatory scrutiny, loss of customers, and expose issuer to great liability.

Increased Borrowing Costs

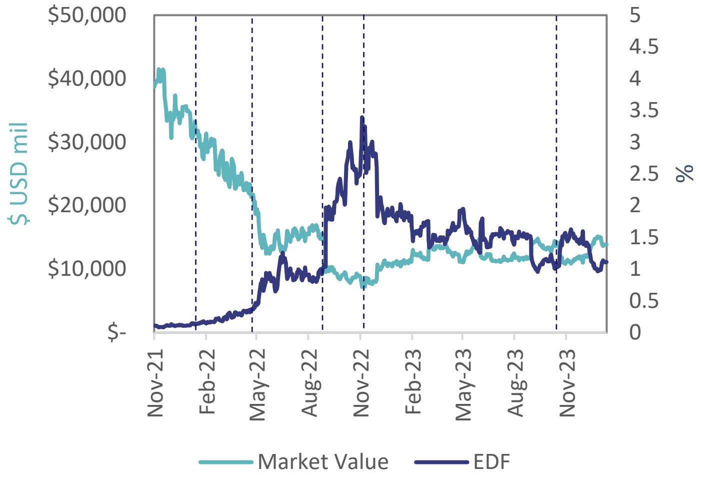
A cyber attack can change the risk profile of an issuer and expose them to higher borrowing costs or more restrictive lending requirements.

Cyber shockwaves: Impact on credit quality

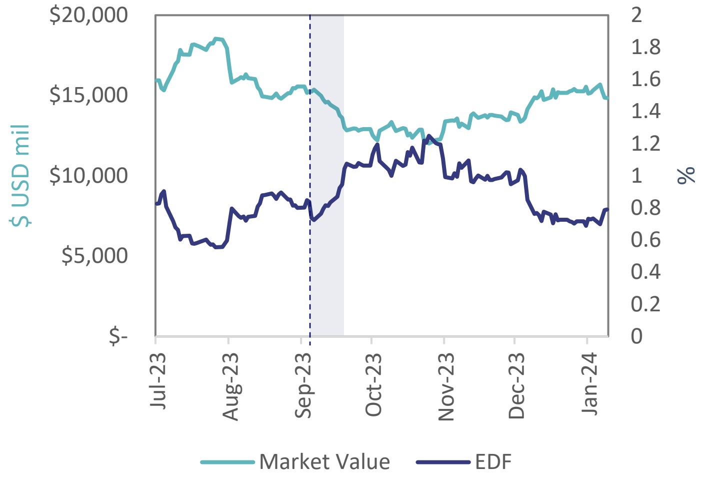
Solarwinds



Okta



MGM



In December 2020, a significant cybersecurity breach involving SolarWinds's software was uncovered.

After filing form 8-K on December 14, 2020, the stock price lost 25% over the next few days and approximately **35%** by the end of the month.

In the same amount of time the PD went from from 0.39% to 0.98%.

The breaches in 2022 and 2023 exposed vulnerabilities in Okta's major clients, impacting market capitalization and credit quality immediately.

Within four months of 2022, Okta lost 40% of its market value and saw its probability of default triple.

By the end of the year the implied forward looking credit rating migrated from shifting from low to substantial risk.

A cyber attack crippled MGM's casino and hospitality operations for 10 days, during that time MGM's value slumped 14% and its forward-looking probability of default increased by 40%. Going from 0.76 to 1.75

From monitoring to risk management

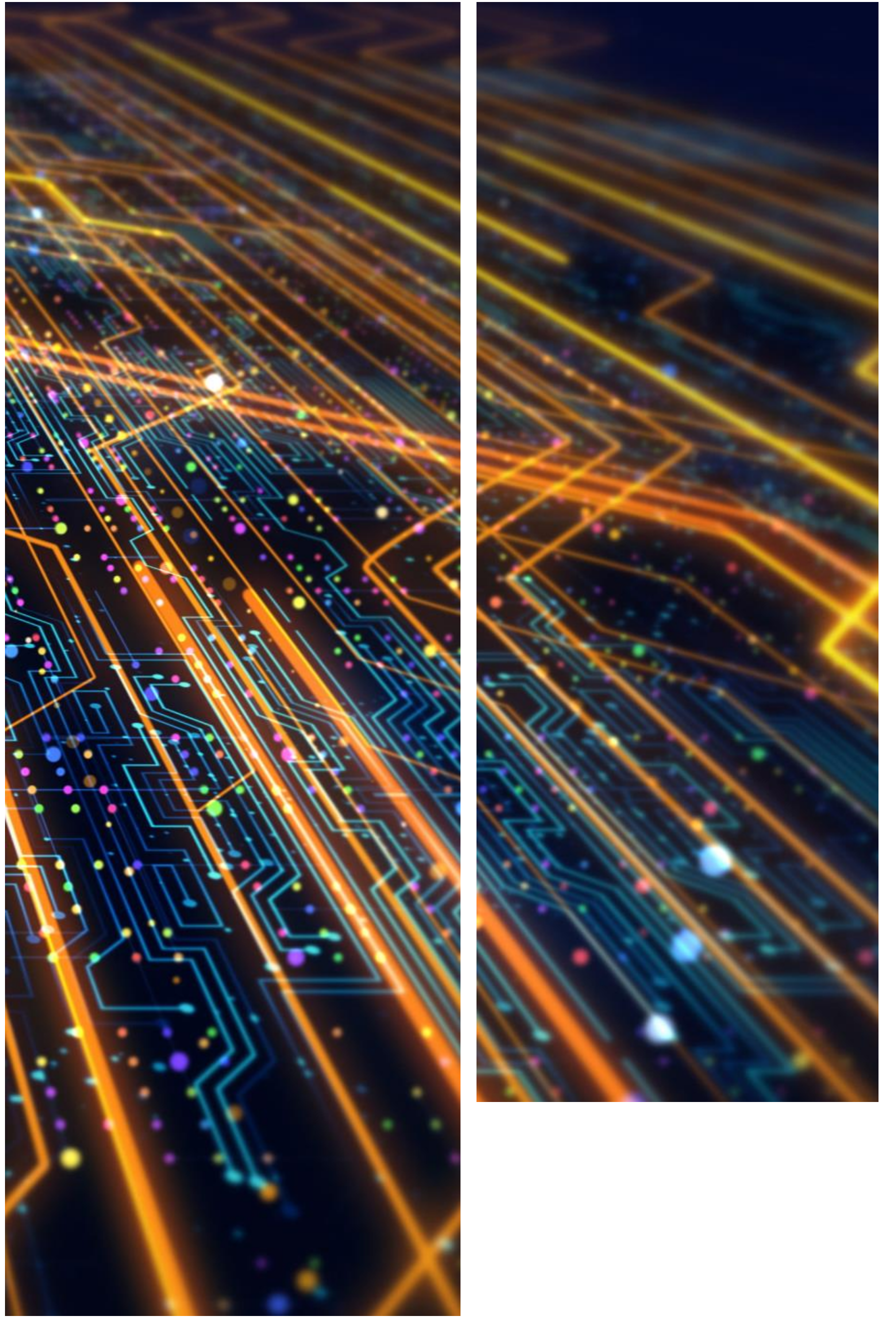
A dual risk model approach

Probability of Cyber Event
What is the firm's probability of observing a cyber event based on their sector, size and score

Expected Loss
For a given event, what is the best reasonable estimate loss from a cyber event

P(Event) x Loss Given Event = Expected Loss

Loss Given Event
If a firm does have an event, what would the loss severity be given risk mitigants.

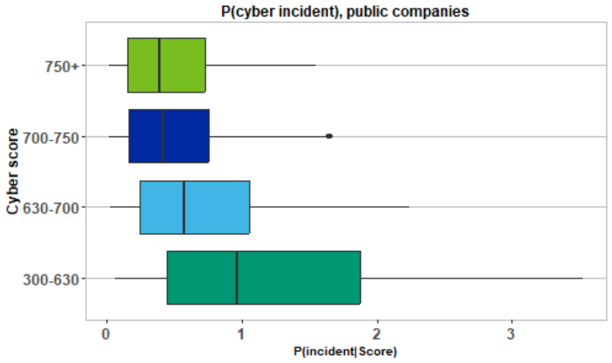


Probability of a cyber event

Takeaways from modeling exercise

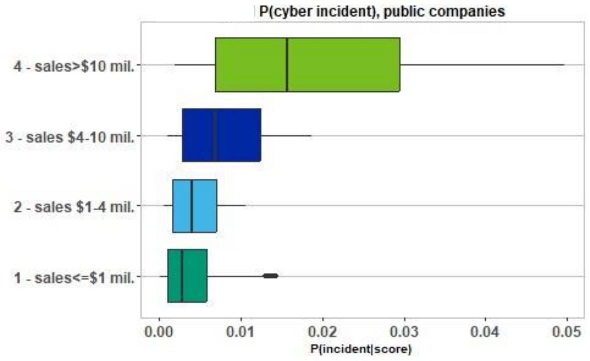
Cyber security practices matter

Companies with good cyber ratings have a lower probability of a cyber event.



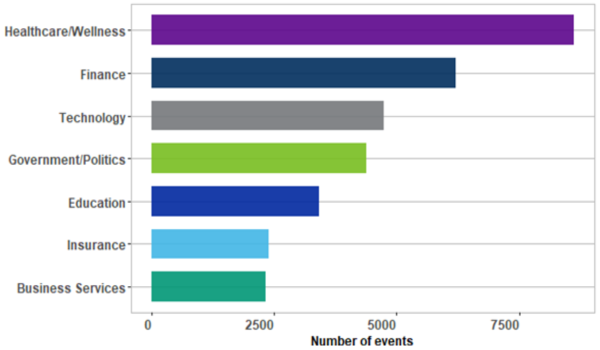
Company size is a good predictor of a cyber event

Larger companies are more likely to be attacked



Information relevance varies across sectors

Probability varies across industries (some sectors are more likely to get impacted than others)



Geography matters

Controlling by country captures different regulatory frameworks.

MOODY'S

Loss Given Event

Assessing the impact on market value after a cyber event

Event study approach (based on seminal paper by Campbell, Lo, MacKinlay, 1997)

Answer questions about how markets perceive and respond to **new information** (ESG controversies, earnings call, new strategy, cyber event, news).

The **Efficient Market Hypothesis** is a foundational assumption. Stock prices should adjust rapidly to new information.

Assume that market participants assess the impact of events on a firm's **expected** future profits.

These assumptions imply that the **expected returns** can be modelled ***h*** periods ahead.

Key concepts

Expected returns: using single factor model based on a firm's beta to market.

$$R_{i\tau} = \alpha_{it} + \beta_{it} MKT_{\tau} + \varepsilon_{i\tau}$$

Abnormal returns is the difference between observed and expected returns.

$$AR_{i,t+h} = R_{i,t+h} - (\hat{\alpha}_{it} + \hat{\beta}_{it} MKT_{t+h})$$

Cumulative abnormal returns aggregate abnormal returns over an event window.

$$CAR_{i,t+2} = AR_{it} + AR_{i,t+1} + AR_{i,t+2} + \ldots$$

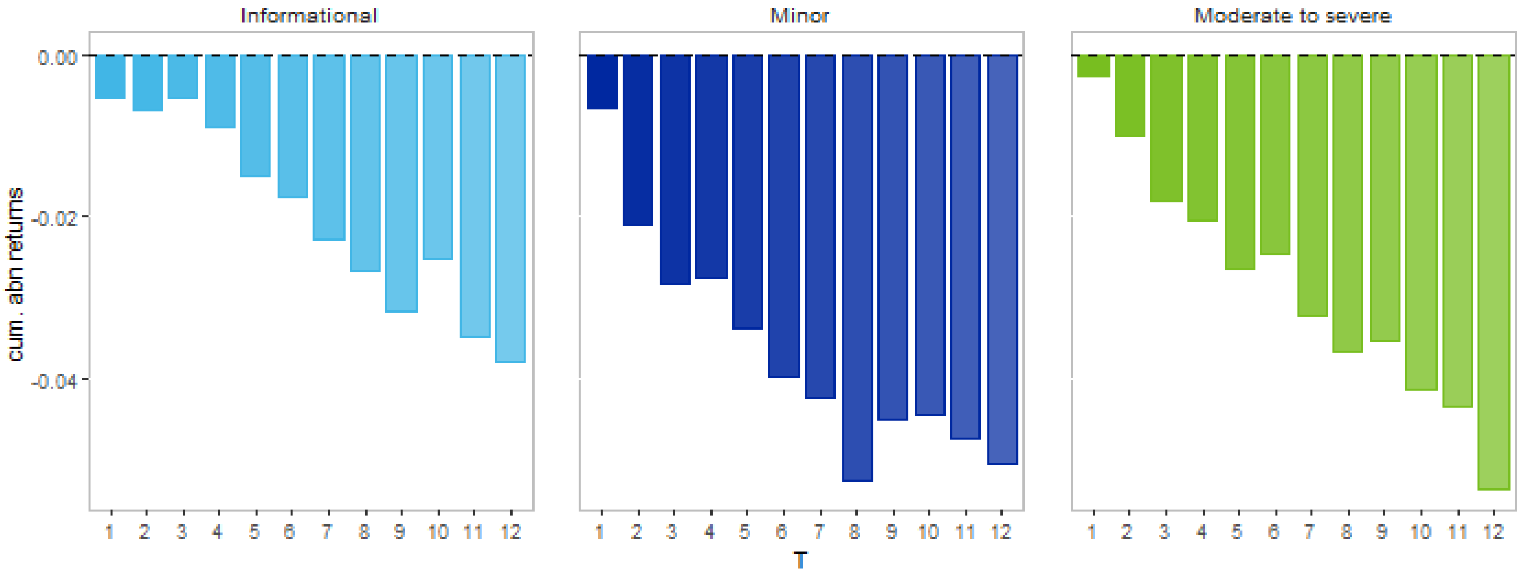
Test: are abnormal returns statistically different from zero? If so, the difference is the **impact** of the event

Impact on market value given a cyber event

- We find the cumulative abnormal returns n months after events reported.
- Ran a statistical test to validate our findings
- Found that cumulative abnormal return are negative and statistically significant.
- Present average losses in terms of returns not levels.

Average cumulative abnormal returns up to 12 months post cyber event by severity

Event type	N	mean	t
	1 - month after incident		
Informational	1,395	-0.54 %	-5.12089
Minor	680	-0.674%	-3.11278
Moderate to severe	1,308	-0.28 %	-2.48496
	2 - month after incident		
Informational	1,377	-0.678 %	-4.48888
Minor	669	-2.084 %	-6.7019
Moderate to severe	1,292	-0.999 %	-6.20012
	12- months after incident		
Informational	1,247	-3.796 %	-9.28625
Minor	610	-5.041 %	-6.0334
Moderate to severe	1,163	-5.352 %	-12.2115



Connecting event analysis to credit risk

Objective: Observe how credit quality changes in the event of a cyber attack.

Structural model based on the Black-Scholes option pricing. Suggests that a company's equity is a call option on the asset value. Probability of Default (PD) is driven by three key elements:

Assets	Market value of assets: inferred from market capitalization
Liabilities	Default point: Threshold for asset value
Volatility	Uncertainty of future cashflows.

- From the abnormal returns described in the event study, we obtain **observed** and **expected** market value.
- Each have an associated **observed** and **expected** PD.
- The difference is the impact on credit risk.
- The Probability of Default at time t is defined as:

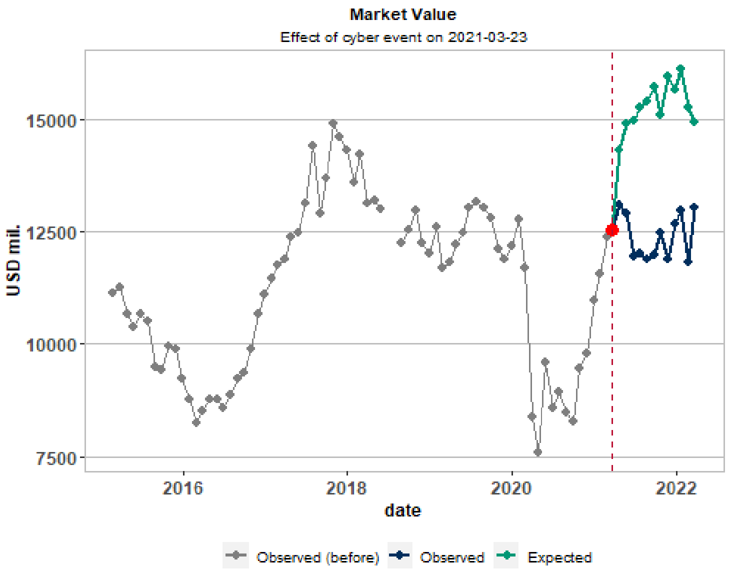
$$PD_t = Pr[A_t \leq D] = Pr[ln(A_t) \leq ln(D)]$$

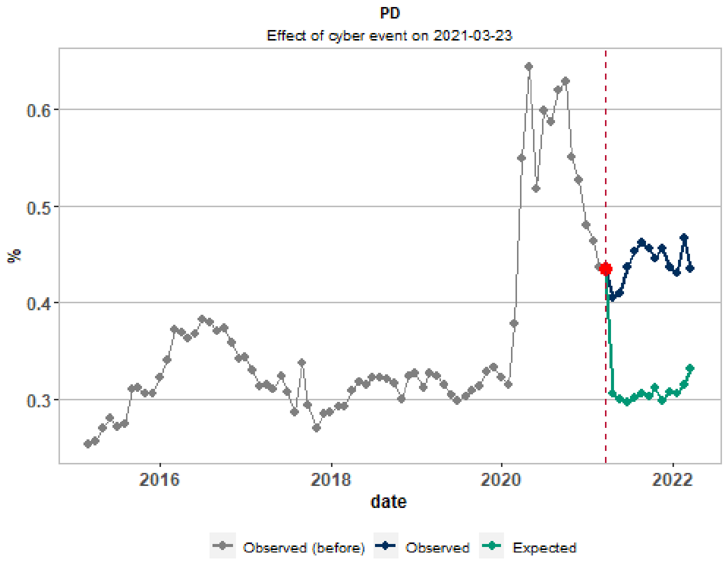
- Market Asset value (A) is unobservable, but we infer it as follows:

$$Asset = Equity + Liabilities - Default\ risk\ premium$$

- Use the volatility of the assets and find the PD using the calibrated function:

$$PD_t = M\left[-\frac{log\left(\frac{A_0}{D}\right)+\left(\mu_A-\frac{1}{2}\sigma_A^2\right)}{\sigma_A}\right]$$





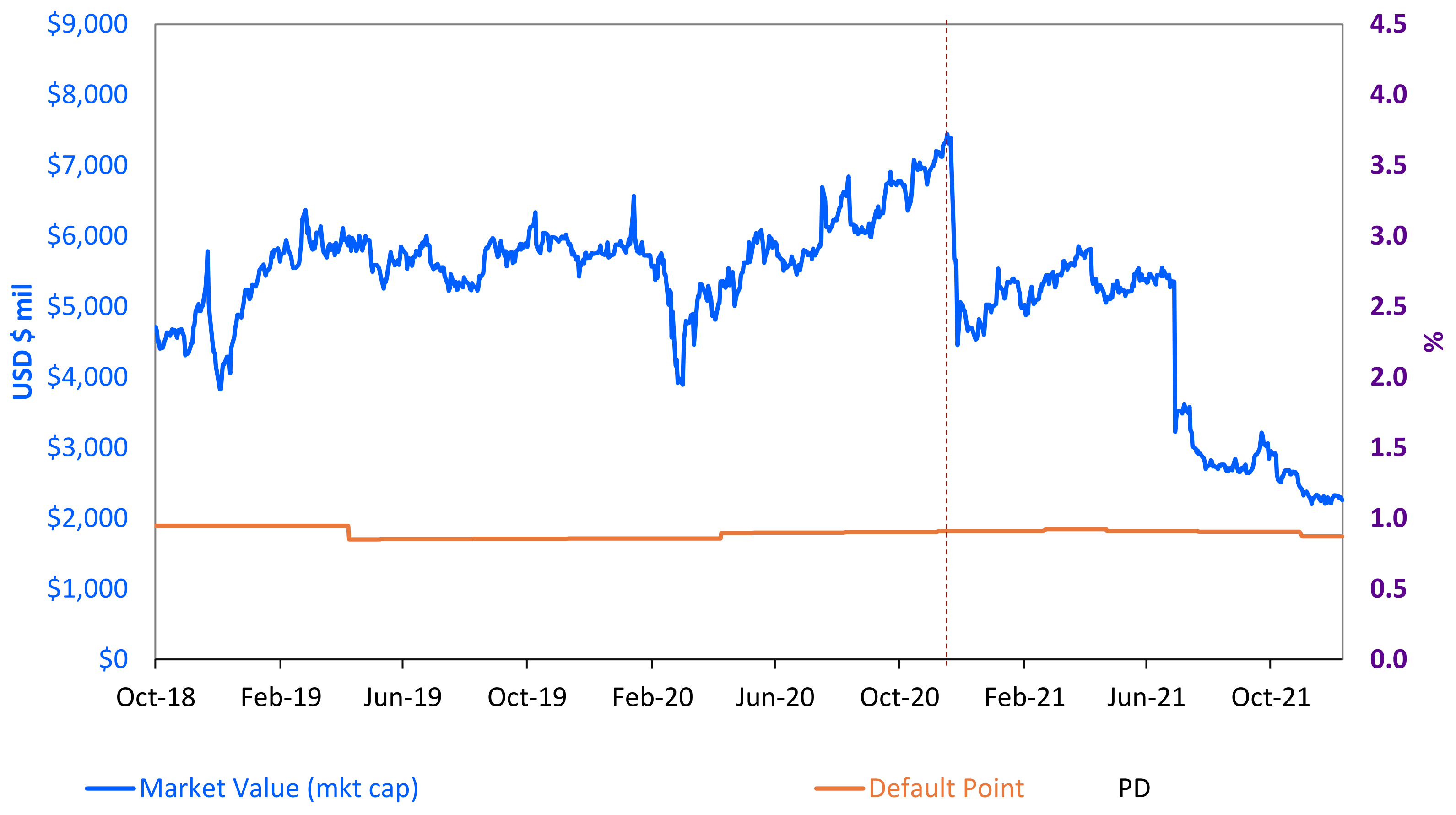
Connecting event analysis to credit risk

Objective: Observe how credit quality changes in the event of a cyber attack.

Structural model based on the Black-Scholes option pricing. Suggests that a company's equity is a call option on the asset value. Probability of Default (PD) is driven by three key elements:

Assets	Market value of assets: inferred from market capitalization
Liabilities	Default point: Threshold for asset value
Volatility	Uncertainty of future cashflows.

Solarwinds



In December 2020, a significant cybersecurity breach involving SolarWinds's software was uncovered. After filing form 8-K on December 14, 2020, the stock price lost 25% over the next few days and approximately 35% by the end of the month.

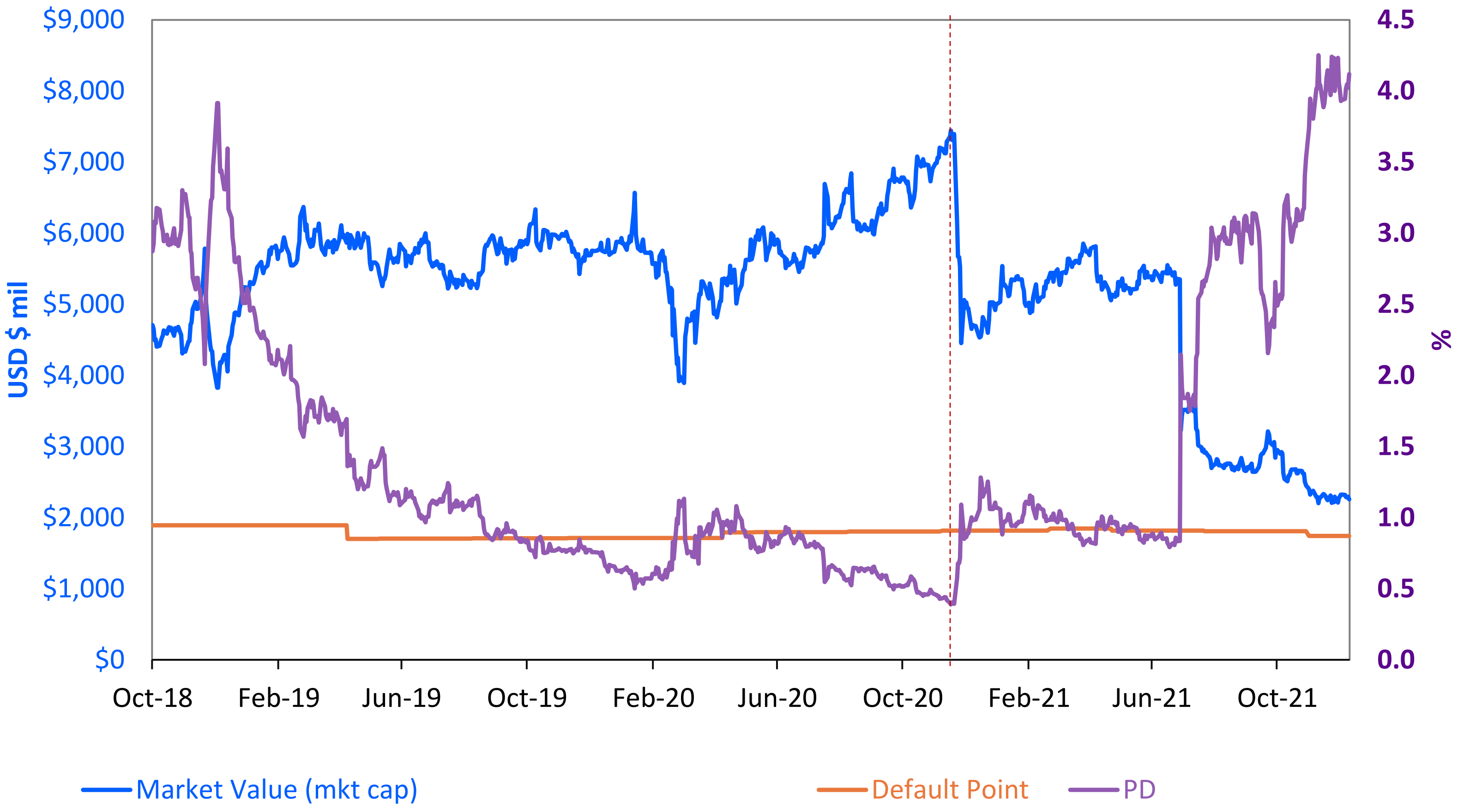
Connecting event analysis to credit risk

Objective: Observe how credit quality changes in the event of a cyber attack.

Structural model based on the Black-Scholes option pricing. Suggests that a company's equity is a call option on the asset value. Probability of Default (PD) is driven by three key elements:

Assets	Market value of assets: inferred from market capitalization
Liabilities	Default point: Threshold for asset value
Volatility	Uncertainty of future cashflows.

Solarwinds



In December 2020, a significant cybersecurity breach involving SolarWinds's software was uncovered. After filing form 8-K on December 14, 2020, the stock price lost 25% over the next few days and approximately 35% by the end of the month.

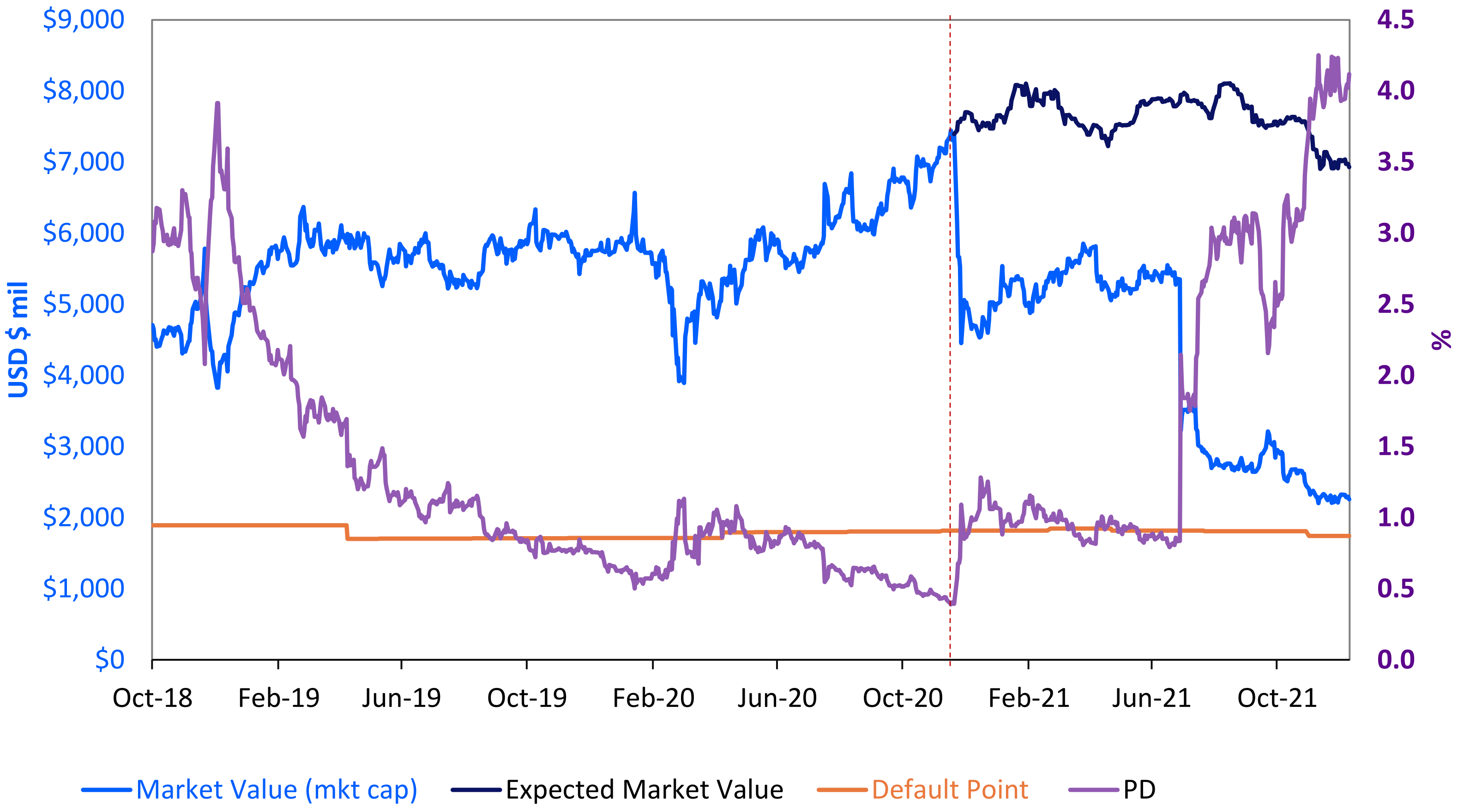
Connecting event analysis to credit risk

Objective: Observe how credit quality changes in the event of a cyber attack.

Structural model based on the Black-Scholes option pricing. Suggests that a company's equity is a call option on the asset value. Probability of Default (PD) is driven by three key elements:

Assets	Market value of assets: inferred from market capitalization
Liabilities	Default point: Threshold for asset value
Volatility	Uncertainty of future cashflows.

Solarwinds



In December 2020, a significant cybersecurity breach involving SolarWinds's software was uncovered. After filing form 8-K on December 14, 2020, the stock price lost 25% over the next few days and approximately 35% by the end of the month.

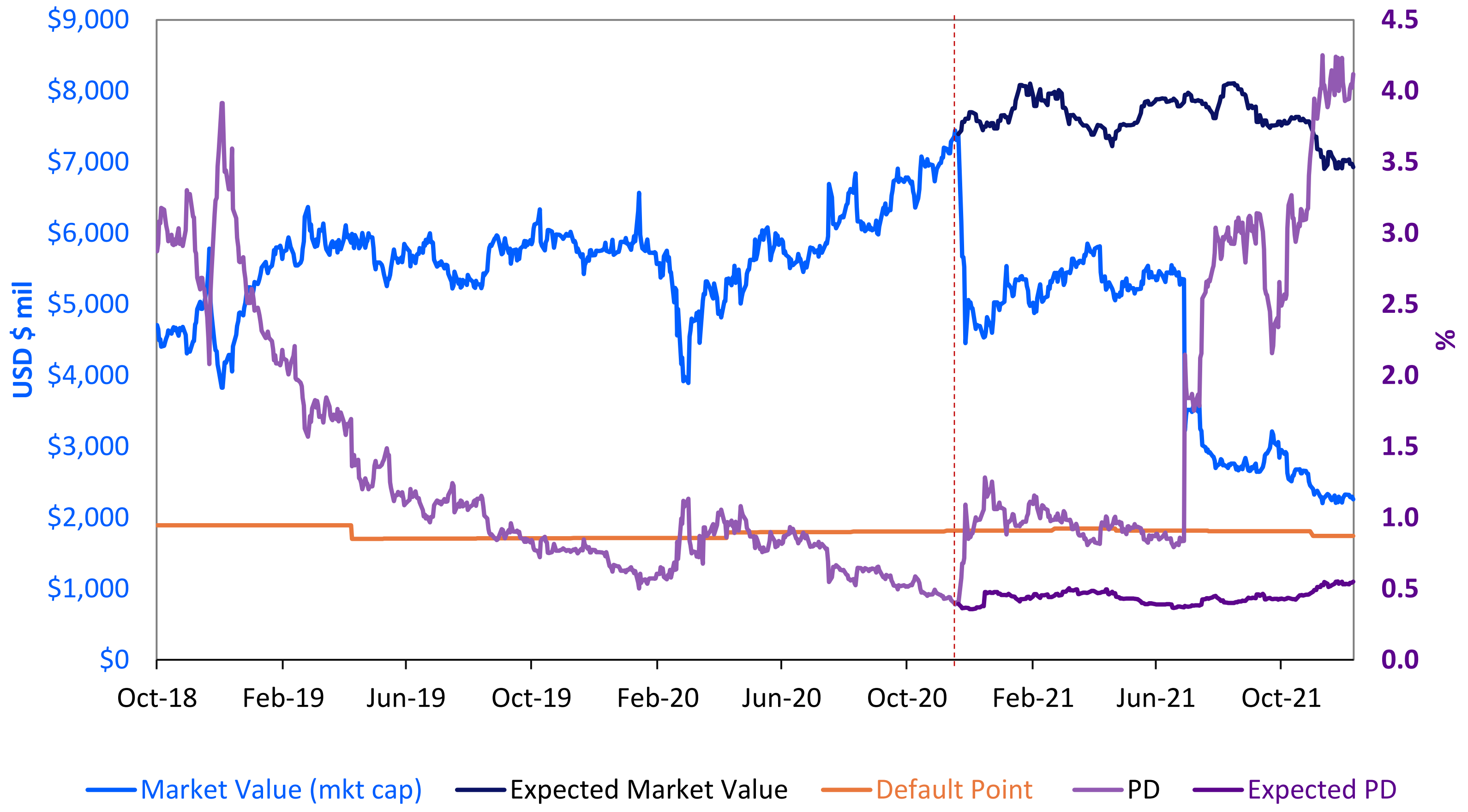
Connecting event analysis to credit risk

Objective: Observe how credit quality changes in the event of a cyber attack.

Structural model based on the Black-Scholes option pricing. Suggests that a company's equity is a call option on the asset value. Probability of Default (PD) is driven by three key elements:

Assets	Market value of assets: inferred from market capitalization
Liabilities	Default point: Threshold for asset value
Volatility	Uncertainty of future cashflows.

Solarwinds



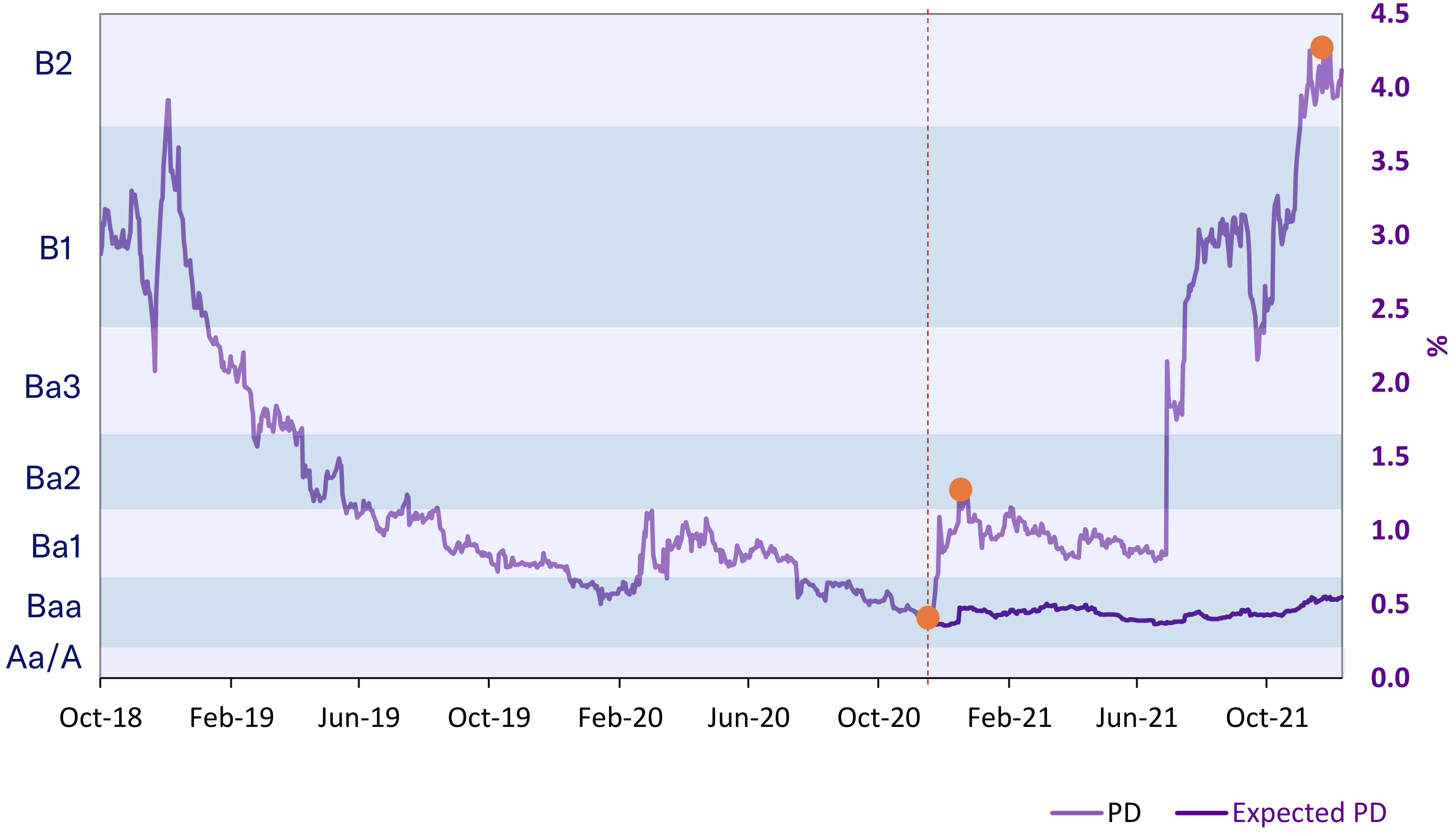
In December 2020, a significant cybersecurity breach involving SolarWinds's software was uncovered. After filing form 8-K on December 14, 2020, the stock price lost 25% over the next few days and approximately 35% by the end of the month.

Connecting event analysis to credit risk

Moody's Implied ratings:

Static Rating Mapping Cutoffs		
Notch	Static Rating	1-yr Cutoff
1	Aaa	0.02%
2	Aa1	0.03%
3	Aa2	0.05%
4	Aa3	0.09%
5	A1	0.14%
6	A2	0.18%
7	A3	0.22%
8	Baa1	0.28%
9	Baa2	0.43%
10	Baa3	0.66%
11	Ba1	1.10%
12	Ba2	1.65%
13	Ba3	2.48%
14	B1	3.71%
15	B2	5.57%
16	B3	8.35%
17	Caa/C	100.00%

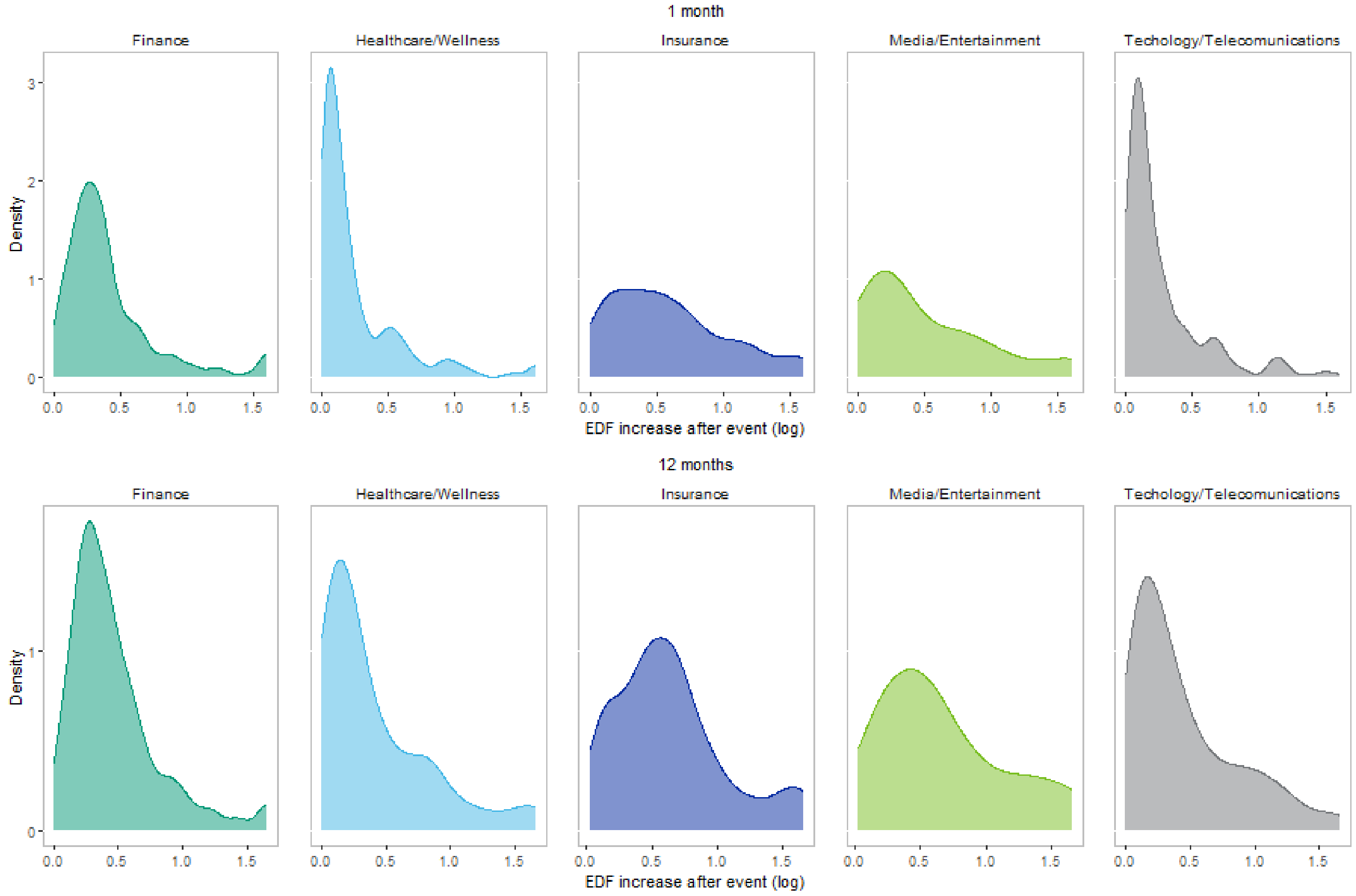
Solarwinds



In December 2020, a significant cybersecurity breach involving SolarWinds's software was uncovered. After filing form 8-K on December 14, 2020, the stock price lost 25% over the next few days and approximately 35% by the end of the month.

Connecting market return to credit risk

Expected vs observed PD after cyber event



- Credit impact varies across industries.
- Sectors observing the largest number of attacks (finance, healthcare and technology) have the lowest increase in PD.
- There is an element of persistence over time, as PD changes increases over time.

Takeaways

Cyber scores matter

→ Cyber hygiene score is predictive of the probability of an attack.

→ Its impact varies across sectors

Data challenges

→ Under reporting diminishes the models' quality

Cyber remains an underpriced area of risk

→ There is a challenge associated to measuring cyber risk, and an opportunity to be included in healthy risk management framework

Financial effect of cyber events tend to be persistent

→ Not all cyber events have a material impact.

→ On average, those that do, have a persistent event over time.

Thank you

Alejandra Caro

Associate Director/
Predictive Analytics

*alejandra.carorincon
@moodys.com*