MOODY'S | Better decisions

Credit Risks in the Face of Cyber and Other Emerging Threats

Amnon Levy, Libor Pospisil – Moody's Analytics
Lesley Ritter – Moody's Investors Service
Derek Vadala – VisibleRisk

June 2021

Moody's (NYSE:MCO) is a global integrated risk assessment firm that empowers organizations to make better decisions. Its data, analytical solutions and insights help decision-makers identify opportunities and manage the risks of doing business with others. We believe that greater transparency, more informed decisions, and fair access to information open the door to shared progress. With over 11,400 employees in more than 40 countries, Moody's combines an international presence with local expertise and more than a century of experience in financial markets. Learn more at moodys.com/about.

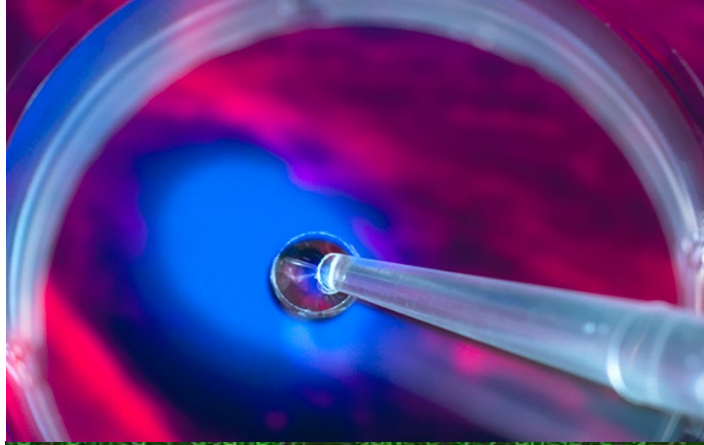
Moody's Corporation is comprised of two separate companies: Moody's Investors Service (MIS) and Moody's Analytics (MA).

Moody's Investors Service (MIS) provides investors with a comprehensive view of global debt markets through credit ratings and research. Moody's Analytics (MA) provides data, analytics, and insights to equip leaders of financial, non-financial, and government organizations with effective tools to understand a range of risks.

© IACPM

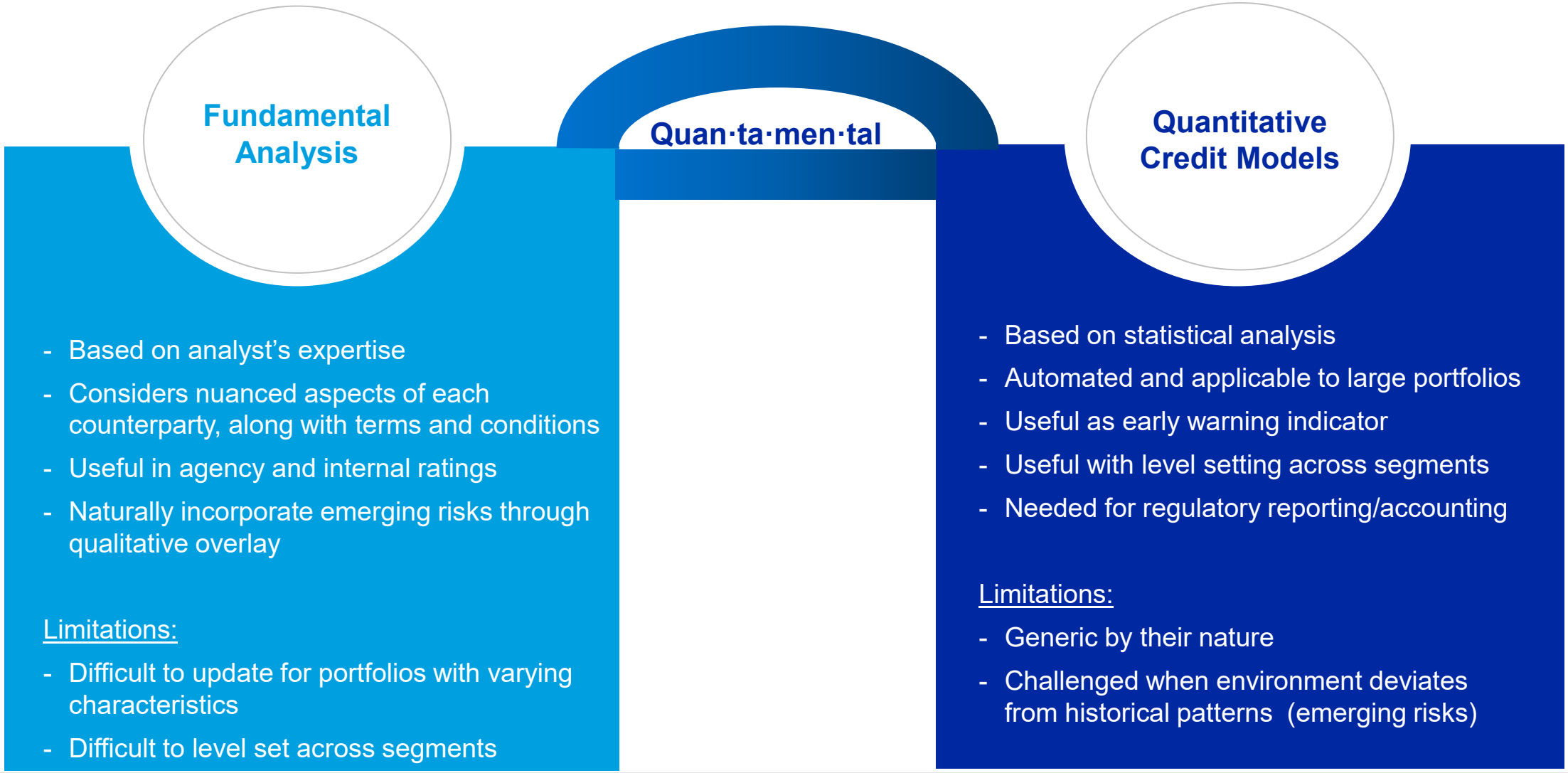
Goals for This Session

- Review the gaps in credit models revealed by the COVID-19 Pandemic
- Outline a cohesive credit risk framework that assesses emerging threats, such as cyber risk and climate hazards
- Review qualitative methods used in fundamental analysis that overcome data challenges inherent in emerging risks
- Use alternative data to describe the varying impact of emerging risks across credit segments
- Live Q&A



Articulating the Impact of Emerging Risks on Credit

In the context of current approaches to modeling of credit



Lessons from Previous Crises

Overcoming challenges with modeling emerging risks

Traditional Quantitative Credit Models

Models used for loss projections, IFRS9/CECL, stress testing.

Based on longer time series of data, at lower frequencies, such as quarterly.

Broad-brush economic variables, unable to differentiate industry impact.

Quantitative Emerging Risks Framework

Credit Risk Data

Higher frequency, name-level data captures cross-sectional patterns by allowing for empirical analysis with segment granularity descriptive of the emerging risk

Alternative Data

Mobility Indexes
Consumer Sentiment
Supply chain
Vulnerability to cyber events
Geo-location of climate hazards

Fundamental Analysis

Emerging risks, by their very nature, are new threats, for which **sufficient historical data does NOT exist**

In many cases, a qualitative assessment can be applied consistently across asset classes and is an indispensable part of risk analysis

The Global Risks Report 2021

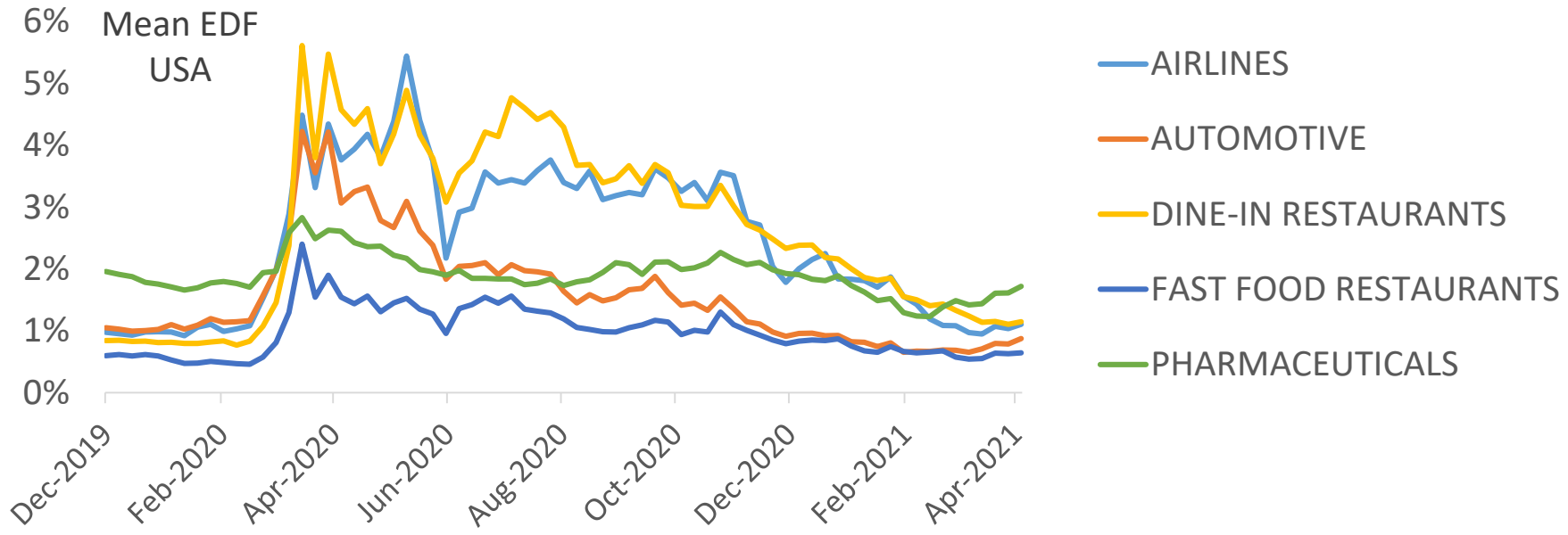
Emerging Threats

WORLD ECONOMIC FORUM

Technological	Geopolitical	Societal	Enviromental
Cyber Events	Supply-Chain Disruption	Trade Disputes	Infectious Diseases	Natural Disasters

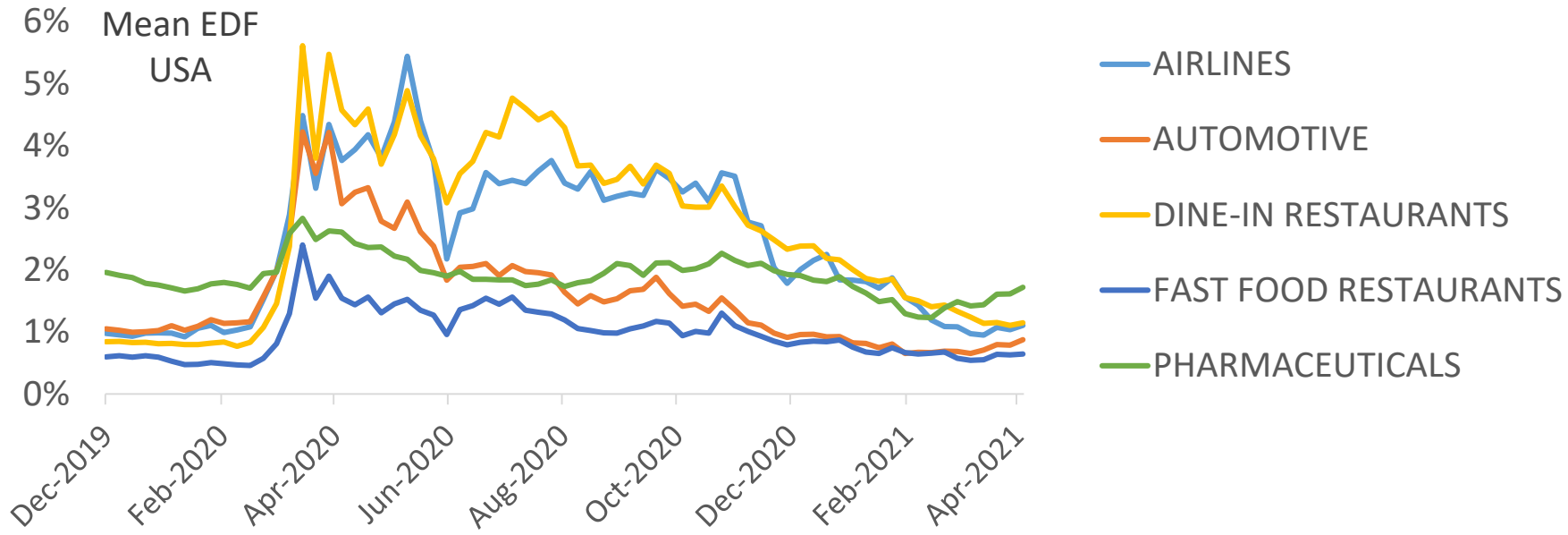
Modeling the Pandemic: Alternative Data

Traditional models cannot capture cross-sectional patterns



Modeling the Pandemic: Alternative Data

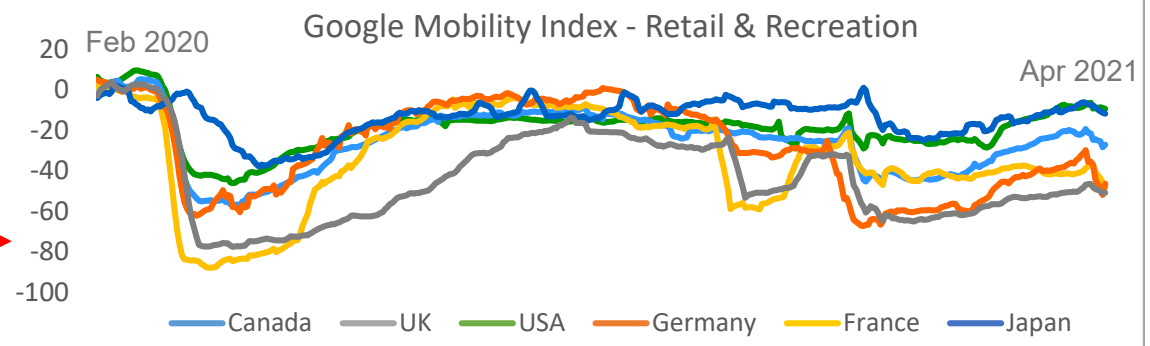
Traditional models cannot capture cross-sectional patterns



How to differentiate dynamics across industry segments?

Calibrate sensitivities of industry segments to measures of

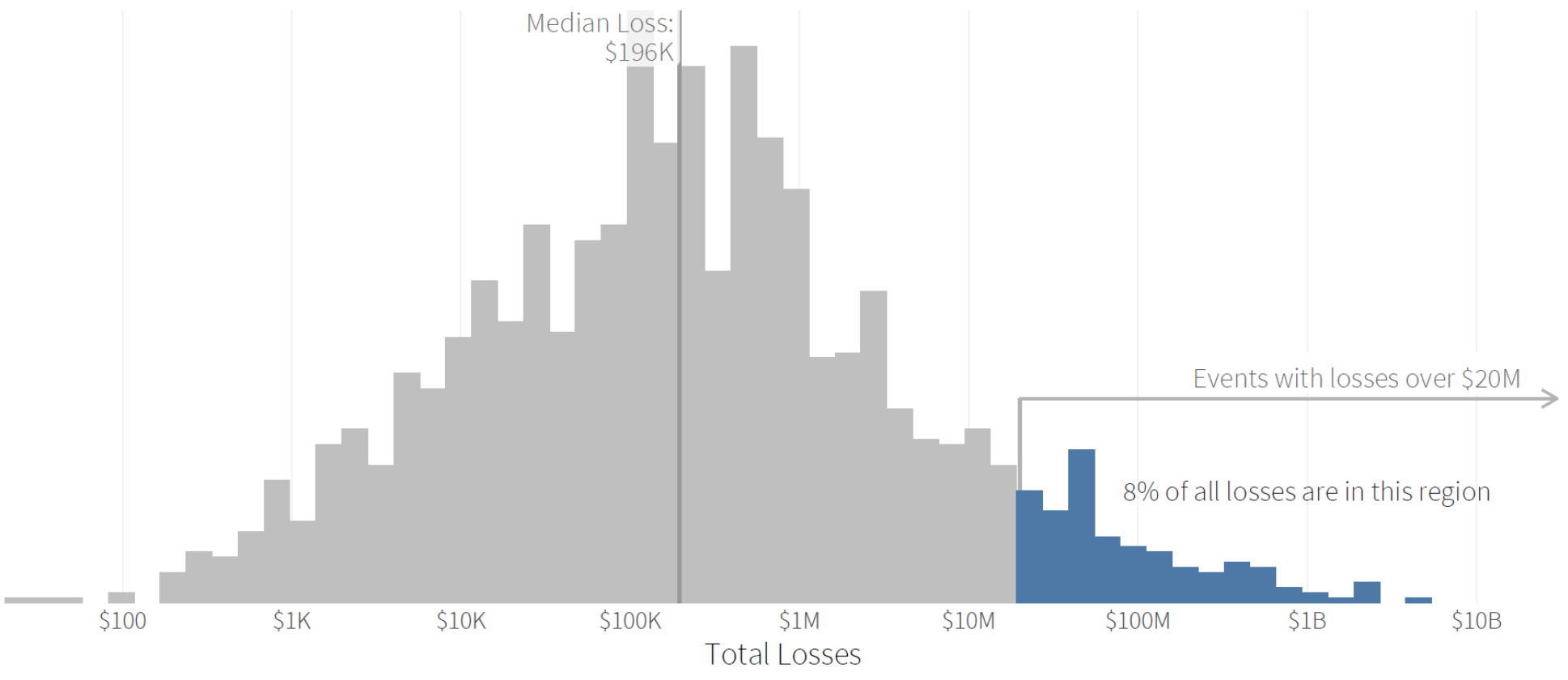
- **Social distancing** & the reaction of the population to the Pandemic… **MOBILITY INDEX**
- **Consumer Sentiment**…Proxied by **EQUITY INDEX**



MOODY'S
INVESTORS SERVICE

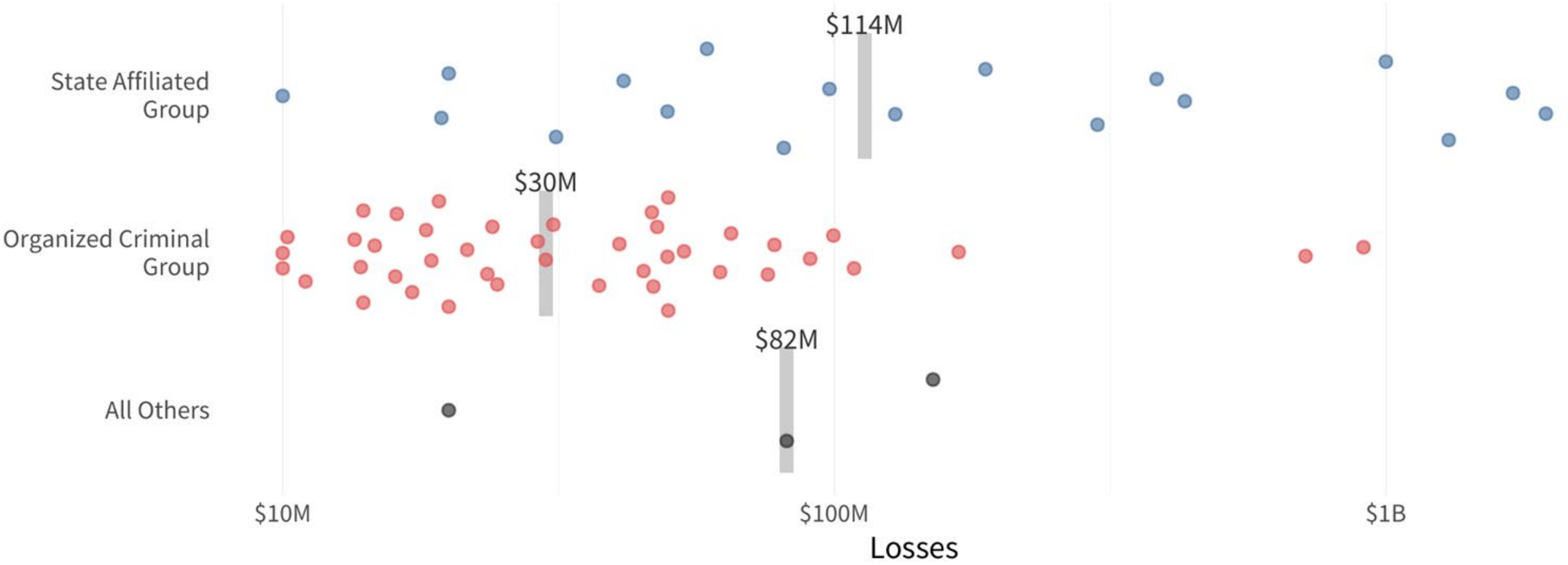
Fundamental Analysis: Bridging the Gap Between Cyber and Credit

We are focused on extreme losses

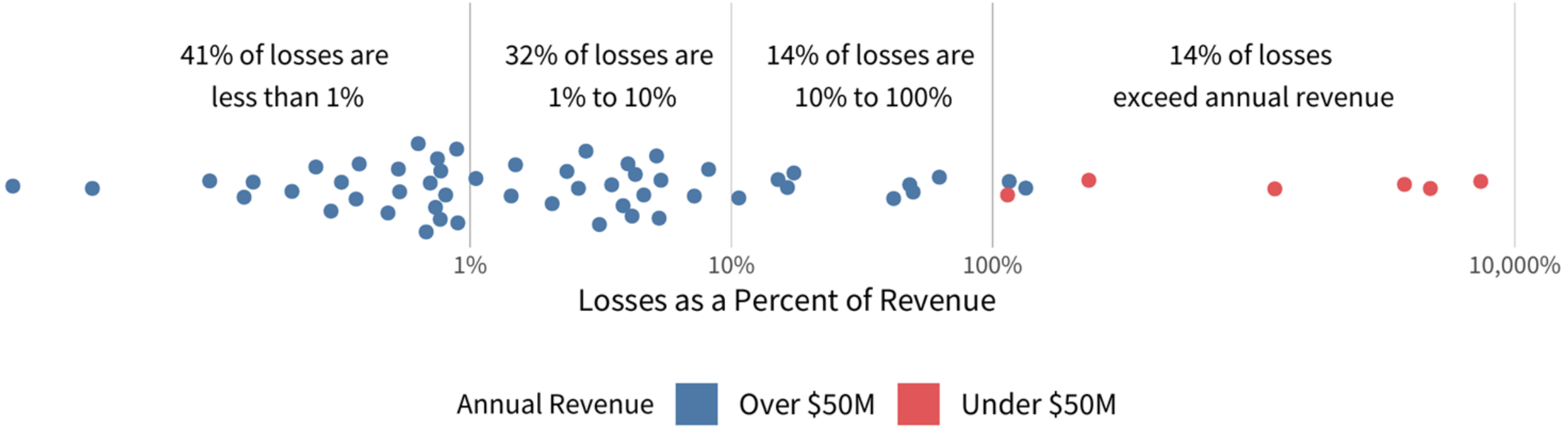


Sources: VisibleRisk and Cyentia Institute

Who are the External Actors?



Losses as a Proportion of Revenue



Attacks on global infrastructure

….becoming more frequent and disruptive

October 2019 –
Attack on India's largest nuclear facility breaches IT network.

March 2020 –
Attack on Europe's Electric Network Transmission Operator breaches IT network.

April 2020 –
Ransomware attack against Energias de Portugal impacts global IT network.

February 2021 –
Eletrobras ransomware attack on IT systems of nuclear power subsidiary.

June 2021 –
JBS halts operations after ransomware attack

Feb 2020 –
Ransomware attack on US natural gas compression facility.

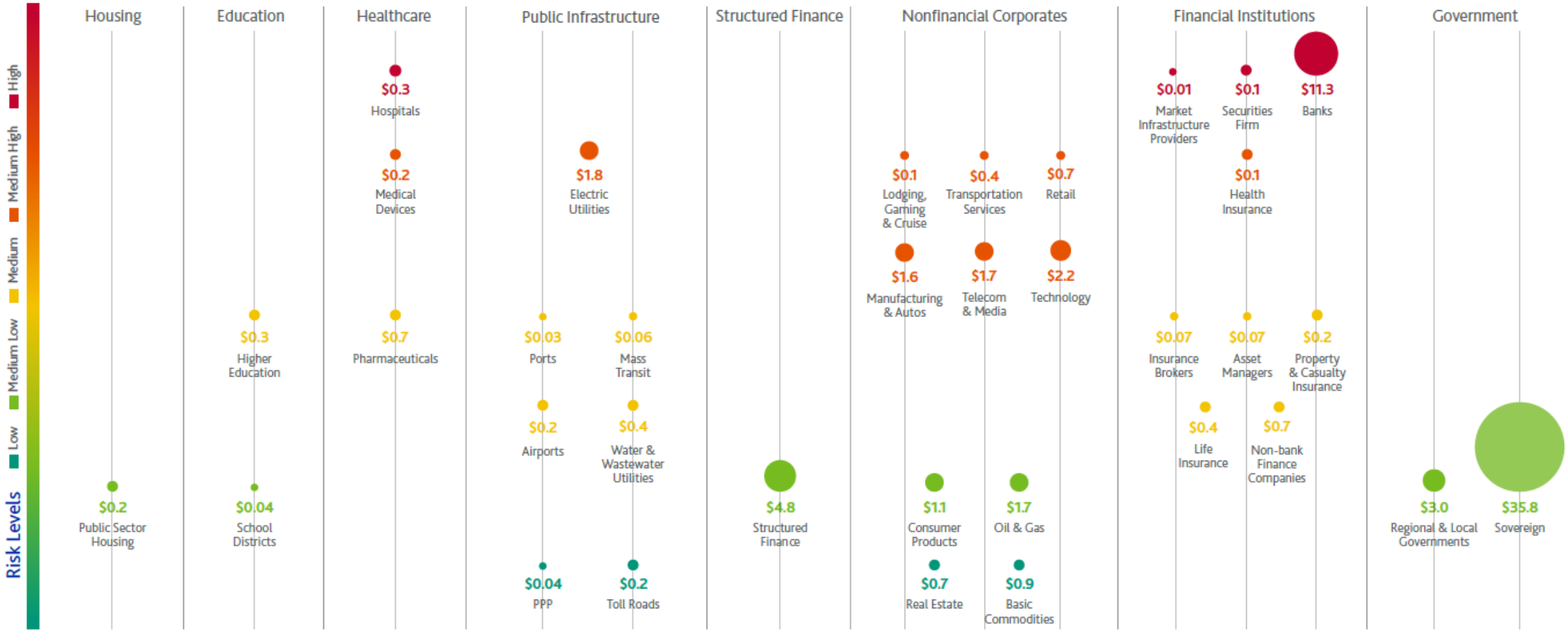
April 2020 –
Attack on Israeli water utility seek to disrupt water supply during COVID epidemic.

June 2020 –
ICS-capable SNAKE ransomware attack launched against Enel disrupt corporate networks

May 2021 –
Colonial pipeline halts operations after ransomware attack on IT systems.

Cyber risk heat map (February 2019)

Cyber risk levels and Moody's-rated debt (in $trillion)

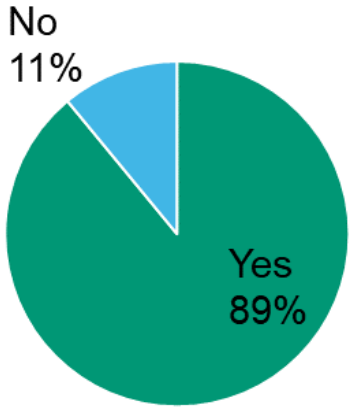


Source: Moody's Investors Service

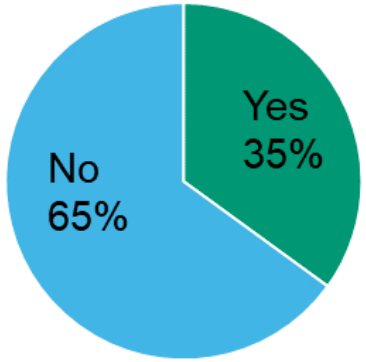
Public disclosures offer little transparency

…..cyber disclosure does not accurately reflect risks, making it hard to incorporate into our credit analysis

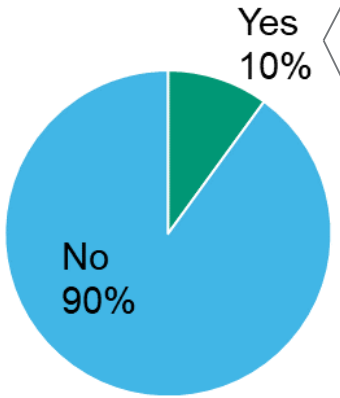
Does company disclose discussion of cybersecurity risk in the annual report or notice of annual meeting?



Does the board identify any board member with cyber security experience?



Does the company disclose a requirement for the CSO to report to the board of directors?



10% breakdown:

The CSO reports directly to the full board (4%)

The CSO reports directly to a board committee that is at least 75% independent (4%)

The CSO does not report in person at formal board or committee meetings (2%)

397 total responses

Proprietary issuer data provides unique insight

….36% response rate achieved during a pandemic!

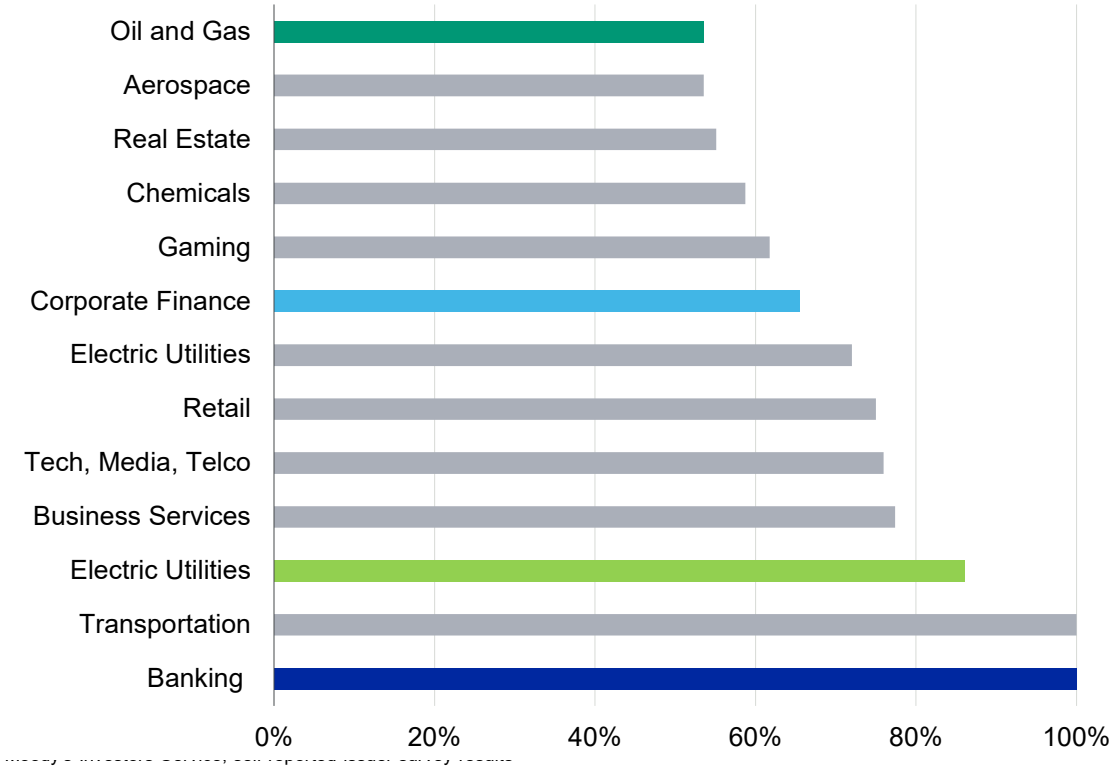
Cyber survey distribution by Rating Group

LOB	Surveys Sent	Surveys Received	% Received	Surveys Declined	% Declined
Financial Instit.	412	200	49%	29	7%
Corporate	2,315	648	28%	82	4%
Infrastructure	342	160	47%	19	6%
SubSov&Pub Fin	677	177	26%	10	1%
Sovereign	125	51	40%	6	5%
Structured Fin	60	16	27%	2	3%
Total	**3,931**	**1,252**	**32%**	**148**	**4%**

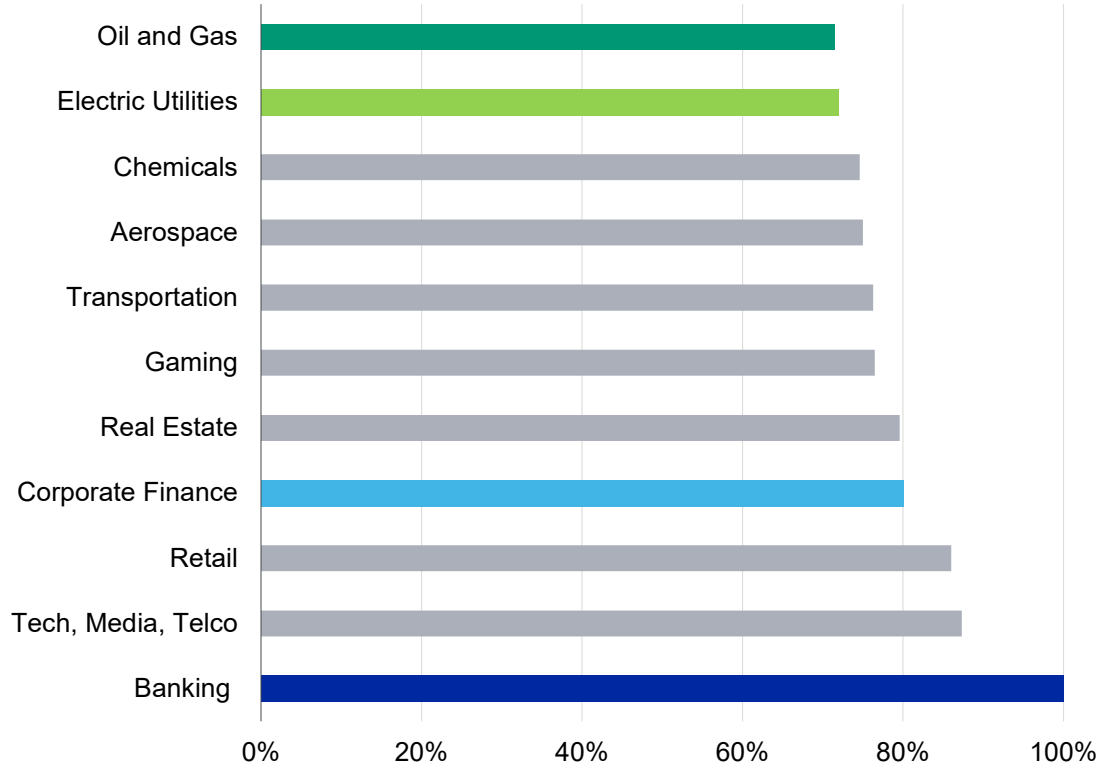
Cyber survey case study – oil & gas

Oil and gas companies less likely to have completed tabletop simulation exercises and cyber assessments of third-party vendors than corporate and banking peers

Percent of respondents by sector that have completed tabletop simulation exercises since May 2020



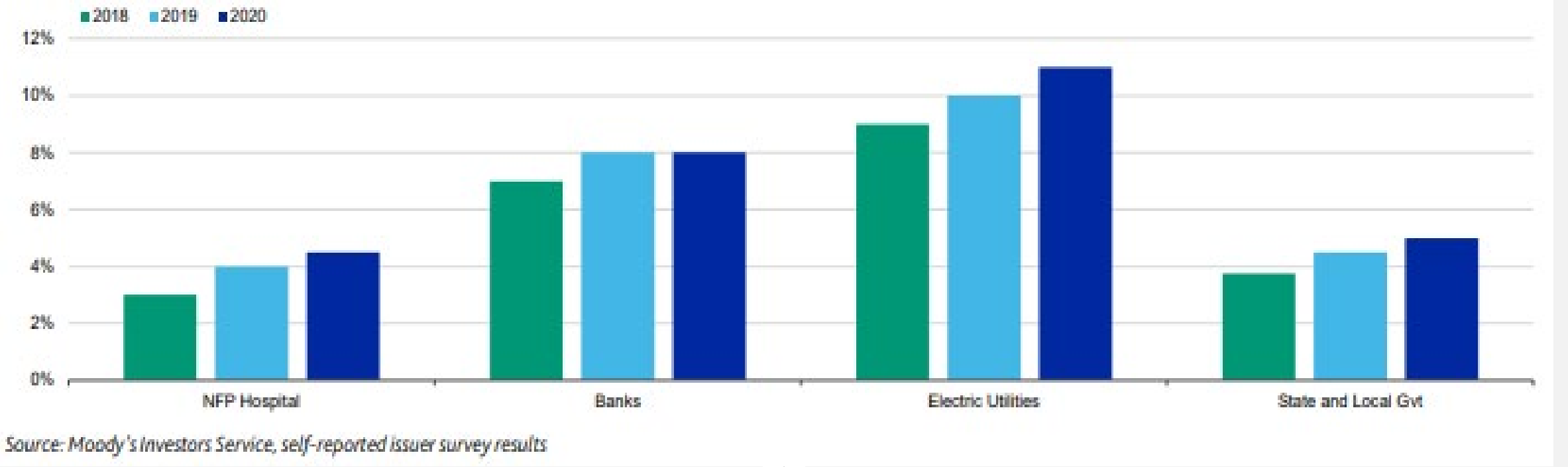
Percent of respondents by sector requiring cyber assessment of third-party vendors



Cyber survey case study – healthcare

Healthcare issuers' investment in cybersecurity is on par with state and local governments' but trails other infrastructure sectors

Percent of total information technology budget allocated to cybersecurity



Source: Moody's Investors Service, self-reported issuer survey results

Meet stakeholder demand

In depth, cyber survey based sector reports gives issuers and investors a unique benchmarking tool to hone their cyber analytical capabilities.

INFRASTRUCTURE AND PROJECT FINANCE

Moody's INVESTORS SERVICE

SECTOR IN-DEPTH

4 November 2020

Rate this Research

TABLE OF CONTENTS

Key takeaways from the survey 5
Detailed survey results 10
Results by size of total assets 10
Results by business model 13
Results for midsize and small utilities (regulated versus not-for-profit) 16
Results comparing vertically integrated utilities and transmission networks 18
Results comparing state-owned and privately owned utilities 21
Results by region 22
Results by rating level 23
Appendix 23
Moody's related publications 26

Contacts

Cintia Nastina +1.212.553.1631
Associate Lead Analyst
cintia.nastina@moodys.com

Lesley Ritter +1.212.553.1607
VP-Senior Analyst
lesley.ritter@moodys.com

Philip Zielke 212-553-0311
Associate Analyst 3
philip.zielke@moodys.com

Leroy Terrelonge 1.212.553.2816
AVP-Cyber Risk Analyst
leroy.terrelonge@moodys.com

Jim Hempstead +1.212.553.4516
MD- Global Infrastructure & Cyber Risk
james.hempstead@moodys.com

Michael Rowen +1.212.553.4463
MD-Glbl Pub Proj and Infra Fin
michael.rowen@moodys.com

» Contacts continued on last page

Electric Utilities – Global

Cybersecurity readiness depends on scale, business model and generation ownership

To see how well electric utilities are prepared to defend themselves from cyberattacks, we conducted a survey of global electric utilities and power companies from March through September of this year. The results reflect key differences across what is otherwise a largely homogeneous sector. All observations in this report are based on our survey results and do not represent a definitive assessment of cybersecurity readiness.

- **Amid growing cyberattacks, survey results reveal disparities in levels of preparedness.** Cybersecurity readiness tends to be stronger among large, regulated utilities than among small utilities and those operating in competitive markets. There appears to be little difference among issuers based on geographic location or rating level.
- **Greater financial resources give very large utilities an edge over smaller counterparts.** Very large utilities exhibit better cyber governance, and risk management practices than midsize and small utilities.
- **Regulated utilities appear better positioned than unregulated and not-for-profit utilities.** Regulated utilities operate critical infrastructure assets and are often judged by their reliability in addition to their profits. As a result, regulators provide cost recovery mechanisms designed to maintain well-rounded cybersecurity practices.
- **Among midsize and small utilities, cyber insurance helps mitigate weaker resiliency practices of not-for-profit utilities.** Not-for-profit utilities with total assets of less than $10 billion are more likely to have stand-alone cyber insurance and derive greater coverage value from their policy than similarly sized, regulated peers.
- **Cybersecurity readiness is stronger among vertically integrated utilities than transmission networks.** Vertically integrated utilities display stronger cybersecurity readiness, with closer links between cyber managers and the corporate executive team, a more diverse and sophisticated arsenal of cyber defense practices and more prevalent adoption of cyber insurance.
- **Use of advanced cyber practices are more common at privately owned than state-owned utilities.** But utility types rely on similar cyber risk governance practices and are investing in cybersecurity at about the same rate.
- **Rating levels and regional differences are not major distinguishing factors.** Cybersecurity readiness does not differ significantly by rating or region, but there are some differences in terms of cyber employee headcounts and cyber insurance coverage.

FINANCIAL INSTITUTIONS

Moody's INVESTORS SERVICE

Global Cyber Risk Issuer Surveys

SECTOR IN-DEPTH

2 March 2021

Rate this Research

TABLE OF CONTENTS

North American banks have generally strong cyber risk practices 2
Key take-aways from the survey 3
Rating level does not reveal meaningful differences 8
Moody's related publications 9

Contacts

Megan Fox +1.212.553.4986
AVP-Analyst
megan.fox@moodys.com

Siri Ginjupalli +1.212.553.3803
Associate Analyst
siri.ginjupalli@moodys.com

Alessandro Roccati +44.20.7772.1603
Senior Vice President
alessandro.roccati@moodys.com

Leroy Terrelonge 1.212.553.2816
AVP-Cyber Risk Analyst
leroy.terrelonge@moodys.com

Lesley Ritter +1.212.553.1607
VP-Senior Analyst
lesley.ritter@moodys.com

Andrea Usai +1.212.553.7837
Associate Managing Director
andrea.usai@moodys.com

M. Celina Vanoetti +1.212.553.4843
MD-Banking
celina.vanoetti-hutchins@moodys.com

CLIENT SERVICES

Americas 1-212-553-1653
Asia Pacific 852-3551-3077
Japan 81-3-5408-4100
EMEA 44-20-7772-5454

Banks – North America

Cybersecurity strength rests on governance and prevention

To assess North American banks' cyber risk preparedness, we surveyed 29 banks in the region[1]. The results show strong cyber risk practices but with some differences across what is otherwise a largely homogeneous sector. Cyberattacks pose financial, reputational and regulatory risks for banks. Evidence of weak governance, lax risk prevention or poor response and recovery readiness would be credit negative, with the implications of a successful attack reflecting its nature, severity and duration. All observations in this report are based on our survey results and do not represent a definitive assessment of cybersecurity readiness.

- **Cyber governance is typically more robust at larger banks, Canadian banks and US government-related issuers (GRIs).** Large banks[2] and Canadian banks also report greater use of advanced cyber practices. Resource allocation is more substantial at banks where the chief information security officer (CISO) reports directly to the C-suite.
- **Most bank cybersecurity managers report directly to the C-suite,** which raises awareness and understanding of cyber risk. Most banks report at least one board member with cyber credentials, but large banks have more board-level expertise than mid-size and small banks. Canadian banks and US GRIs report to boards on cyber more frequently than US regional banks.
- **Head count and budget allocated to cybersecurity continue to grow.** Growth in head count has coincided with material investment to help ensure that banks' digitalization efforts are secure. There is higher growth in full-time cyber employees and cyber budgets at banks where the CISO reports directly to the C-suite.
- **Advanced cyber defense practices are in wide use.** These include sophisticated exercises like red team testing, with formal processes to remediate findings. Sophisticated practices are more common among large banks and Canadian banks.
- **Cyber risk assessments for external suppliers are also widely adopted.** These include periodic review and timely notification of cybersecurity incidents, vulnerabilities, patches and malware affecting suppliers, highly relevant in light of the Sunburst attack.
- **Cyber risk transfer is extensive and mitigates financial harm.** About 90% of respondents have standalone cyber insurance with extensive coverage, including business interruption, legal settlements, regulatory fines and ransom payments.
- **Cloud adoption will grow.** Cloud technology, which can be more secure, is used the most by Canadian banks and small banks.

FINANCIAL INSTITUTIONS

Moody's INVESTORS SERVICE

Global Cyber Risk Issuer Surveys

SECTOR IN-DEPTH

23 March 2021

Rate this Research

Contacts

Michael Dion, CFA +1.212.553.1887
VP-Senior Analyst
mike.dion@moodys.com

Rokhaya Cisse, CFA +1.212.553.5870
AVP-Analyst
rokhaya.cisse@moodys.com

Yong Kang, CFA +852.3758.1529
Associate Analyst
yong.kang@moodys.com

Alec Johnson +1.212.553.2879
Associate Analyst
alec.johnson2@moodys.com

Lesley Ritter +1.212.553.1607
VP-Senior Analyst
lesley.ritter@moodys.com

Sarah Hibler +1.212.553.4912
Associate Managing Director
sarah.hibler@moodys.com

Marc R. Pinto, CFA +1.212.553.4532
MD-Financial Institutions
marc.pinto@moodys.com

CLIENT SERVICES

Americas 1-212-553-1653
Asia Pacific 852-3551-3077
Japan 81-3-5408-4100
EMEA 44-20-7772-5454

Insurers, Insurance Brokers and Asset Managers — Global

Survey signals cybersecurity strength, with some differences across sectors, regions

To assess insurers', insurance brokers' and asset managers' cyber risk preparedness, we surveyed 100 companies across North America and internationally, primarily in Europe[1]. The results indicate cybersecurity strength, as was the case for North American banks, but with some differences across sectors and regions. Cyberattacks pose financial, reputational and regulatory risks for insurers, insurance brokers and asset managers. Evidence of weak governance, lax risk prevention or poor response and recovery readiness would be credit negative, with the implications of an attack depending on its nature, severity and duration. All observations in this report are based on our survey results and do not represent a definitive assessment of cybersecurity readiness.

Cyber governance is generally stronger at larger insurers, which report greater use of advanced cyber governance practices. North American insurers also reported higher use of advanced practices than did international insurers.

Smaller to medium-sized asset managers' cyber preparedness has matured but lags that of insurers. Respondents reported cybersecurity governance, management and overall cyber preparedness that is more in line with smaller insurers.

Most cybersecurity managers report directly to the C-suite, increasing companies' awareness and understanding of cyber risk. Larger insurers and higher-rated companies have more board-level expertise than smaller and lower-rated companies.

Hiring and budget allocated to cybersecurity are growing. Growth in head count has coincided with material investment in cybersecurity.

Advanced cyber defense practices are widespread. These include sophisticated exercises like red team testing, and are most common among larger companies.

Cyber risk assessments for external supply chain providers are nearly universally adopted, and important given the recent Sunburst and Microsoft attacks. North American insurers were more likely to require third parties to carry cyber insurance than were international insurers.

Cyber risk transfer and coverage is widespread and mitigates financial harm. Most North American respondents have standalone cyber insurance, but it is less prevalent outside North America.

Cloud adoption will grow. Cloud technology can be more secure than on-premise data storage, and migration to the cloud will continue, reducing reliance on site infrastructure.

VISIBLERISK

Our vision

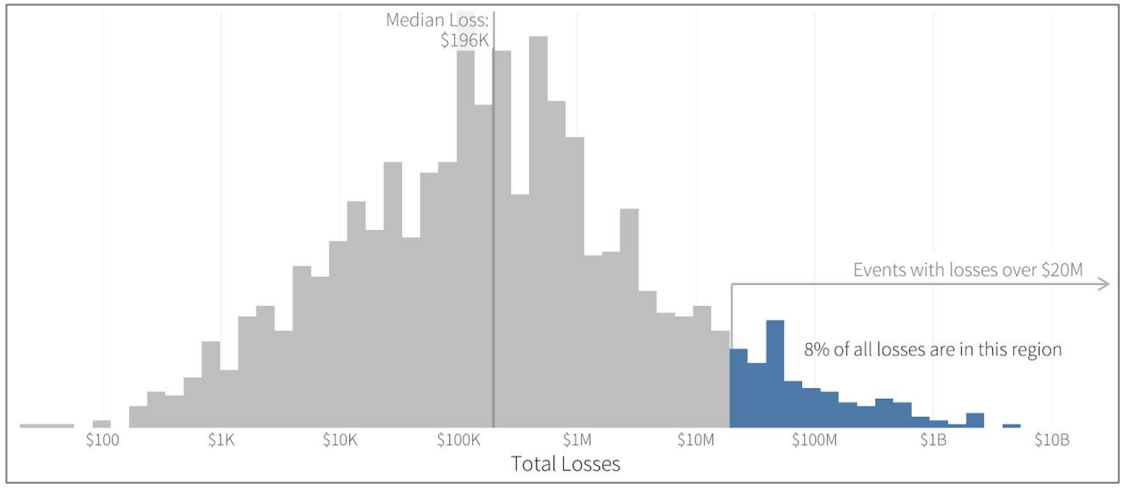
Business leaders should be equipped to understand and confidently manage cybersecurity risk, as clearly as financial risk

A joint venture by TEAM8™ MOODY'S

What is the Challenge?

In 2020, VisibleRisk sponsored a study with the Cyentia Institute that analyzed the 100 largest cyber loss events of the past 5 years. The analysis found:

- The median loss for extreme incidents is $47M, with just over one-in-four exceeding $100M; five events racked up $1B or more in losses.
- Apart from hard costs, 27 events were reported in U.S. Securities and Exchange Commission (SEC) filings, 25 triggered executive changes, and 23 prompted government inquiry.
- Firms that mishandle the incident response process show costs that are nearly 2.8 times larger than those without signs of poor response.



BOARD

Are we fulfilling our governance responsibilities for cyber risk?

Would the loss from a cyber event be material to our company?

CEO

How do we evaluate our security performance? How do we compare to peers?

CFO

Are we spending the right amount on our security program?

CRO

How do we measure and manage cyber risk effectively?

Do we have the right amount and type of cyber risk insurance?

AUDIT

How do we evaluate the efficacy of the security program?

CISO

How can cybersecurity be treated as a business issue?

How can we get the support we need for the security program?

© 2021 Cyber Assessments, Inc. All Rights Reserved. Confidential - Not for Further Redistribution

Threat Capability Evaluation

	Threat Communities		Cyber Capability	
1	**Nation State Attackers**	Privileged Insiders	**Innovative**	These capabilities are the most effective at combating advanced attackers and insiders.
2	**State-Sponsored Cyber Criminals**		**Advanced**	High-performing capabilities that are competitive against the higher grades of attackers an organization may experience including privileged insiders.
3	**Cyber Criminals** (Financial Motivation)	Non-Privileged Insiders	**Intermediate**	Capabilities that are competent at repelling most criminal attacks and insiders.
4	**Cyber Criminals** (Social Motivation)		**Medium**	Capabilities that are somewhat competent at repelling criminal attacks, but good at keeping most non-professionals out (internally and externally).
5	**Opportunists**		**Low**	Capabilities with very little ability to repel attacks, except those that are very unsophisticated.
6	**General Internet Users**		**Very Low**	The least effective capabilities. Typically those that are administrative or policy-only and not supported by automation or technical implementation.

© 2021 Cyber Assessments, Inc. All Rights Reserved. Confidential - Not for Further Redistribution

Rating Formula High Level View

COLLECTED DATA | PEER BENCHMARKING | SCENARIO ANALYSIS | CYBER RISK RATING

Cyber Security Data
- Outside
- Inside
- Intelligence

Business Info
- Financial Profile
- Operational Profile

Security Program
- Surveys
- Interviews
- Benchmarks

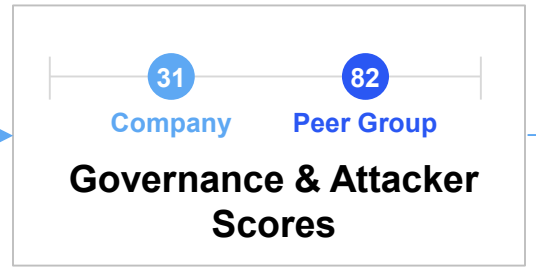
Loss Modeling
- Attack Probability
- Historical Claims Data
- Historical Breach Data

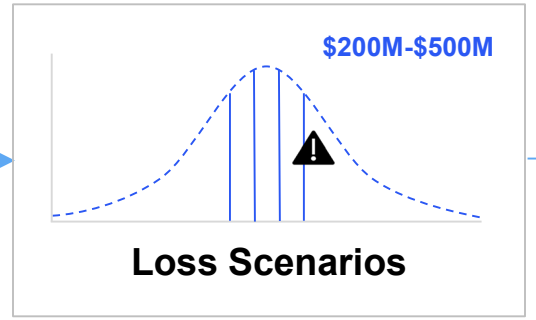
Proprietary Aggregation and Weighting Model

Aggregated metrics are derived from a variety of collected data points and benchmarked against the peer group

Expert Quantification

How companies fare across various metrics dictates where they sit, relative to their peers, in a given loss curve





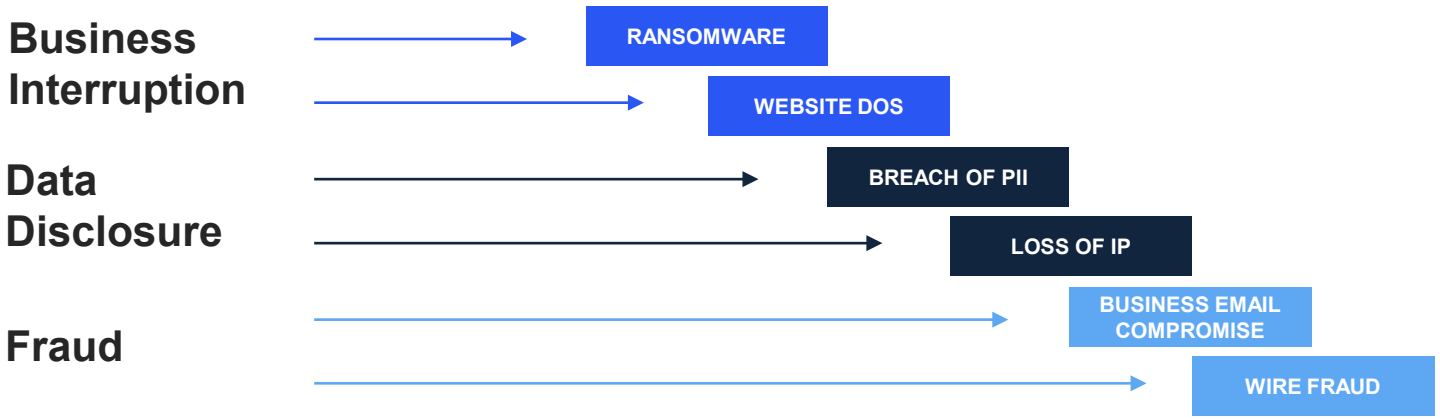
Applied Methodology

CRx

Our rating is based on the results of all risk scenarios, cyber metrics, cultural analyses, budget analyses and threat profile analyses

VISIBLERISK © 2021 Cyber Assessments, Inc. All Rights Reserved. Confidential - Not for Further Redistribution

Cyber Scenario Modeling



Our scenario modeling starts with a series of demographic data points, then aligns them to a sequencing of progressively decomposed scenarios that start at high-level, board-friendly categories and integrates well-known cybersecurity frameworks.

Aligned to Basel II - an internationally recognized ERM framework

Includes mappings to cybersecurity frameworks: MITRE ATT&CK, NIST CSF, CIS, and others

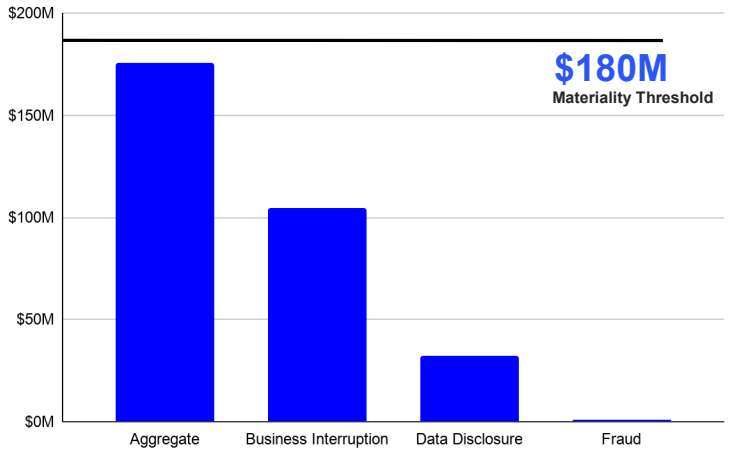
These categories facilitate financial loss conversations around capital allocations, risk tolerance, and cyber insurance

Example detailed mapping from Basel II Framework to MITRE ATT&CK

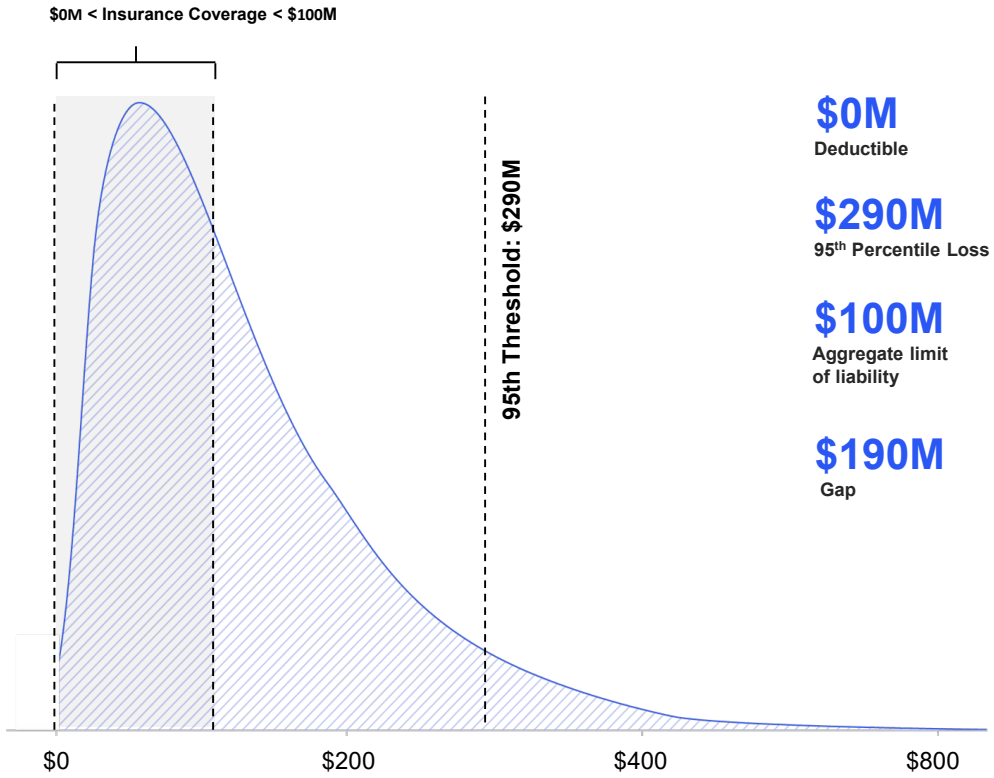
© 2021 Cyber Assessments, Inc. All Rights Reserved. Confidential - Not for Further Redistribution

Materiality and Risk Appetite

This chart shows the difference between cyber losses by type, as an aggregate, taking into account cyber defense and resiliency capabilities. All losses are likely not to exceed the financial materiality threshold ($180M).



This chart takes into account data disclosure, fraud and business interruption aggregate losses at the 95th percentile to the determine The Company's liability.



$0M
Deductible

$290M
95th Percentile Loss

$100M
Aggregate limit of liability

$190M
Gap

Coverage Breakdown

Security and privacy incident expense	✓
Card replacement	✗
Digital asset loss	✗
Cyber extortion	✓
Business interruption and associated costs	✗
Contingent business interruption	✓
Reputational damage	✓
Regulatory fines	✗
Silent Cyber*	✗

© 2021 Cyber Assessments, Inc. All Rights Reserved. Confidential - Not for Further Redistribution

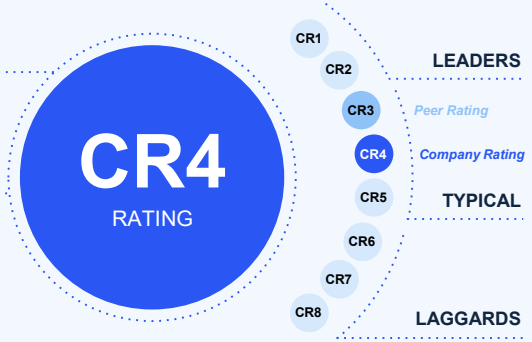
VISIBLERISK

Governance	Risk Mgmt.	Attacker
CR4	CR3	CR5

Exposure

$100M COMPANY

$75M PEER



Insurance Summary

$10M	$100M	$90M
AGGREGATE LIMIT OF LIABILITY	95TH LOSS	GAP

Coverage Breakdown

Security & Privacy Incident Expense ✓	Business Interruption and Associated Costs ✓
Digital Asset Loss ✓	Reputational Damage ✗
Cyber Extortion ✓	Regulatory Fines ✓
Contingent Business Interruption ✓	Silent Cyber ?

Threat Profile

	Threat Communities		Attacker Capability
1	Nation State Attackers	Privileged Insiders ↑	91% to 99%
2	State-Sponsored Cyber Criminals		80% to 97%
3	Cyber Criminals (Financial Motivation)	Non-privileged Insiders ↑	70% to 85%
4	Cyber Criminals (Social Motivation)		50% to 75%
5	Opportunists		40% to 70%
6	General Internet Users		0% to 40%

Business Interruption

Company has approximately $25M of exposure due to cyber disruption events.

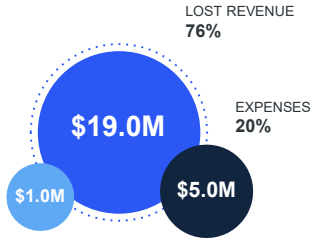
Brand Reputation Impact

LOW | **MED** | HIGH

Compliance Impact

LOW | **MED** | HIGH

Exposure
$25M



Data Disclosure

Company has approximately $15M of exposure due to disclosure of Privacy Information.

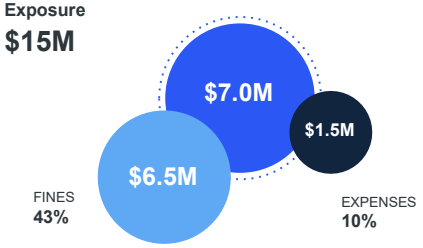
Brand Reputation Impact

LOW | MED | **HIGH**

Compliance Impact

LOW | **MED** | HIGH

Exposure
$15M



Fraud

Company has approximately $5M of fraud exposure largely due to gaps in financial controls associated with invoice processing.

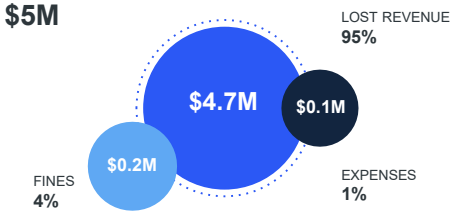
Brand Reputation Impact

LOW | **MED** | HIGH

Compliance Impact

LOW | **MED** | HIGH

Exposure
$5M



Culture of Security

Outcome

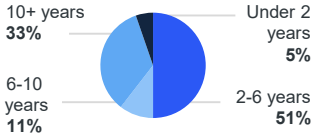
EMERGING | ESTABLISHED | **OUTPERFORM**

Span of Control

3.3 Risk Management Dep

4.28 Security Team

6.88 Information Technology

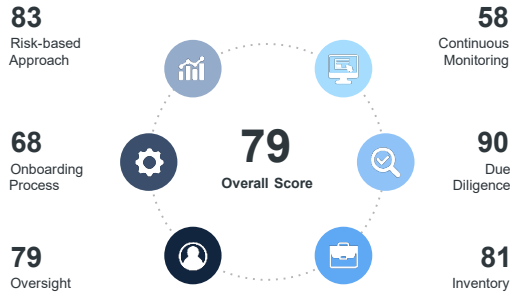


Steps to CEO

1 → 2 → 3

CEO | CRO | CISO

Third Party Risk



Investment

Total budget in comparison to tech budget

Red Team Testing
Sufficient budget allocated to conduct formal and reoccurring red team tests

EDR Product
Sufficient budget allocated to deploy and operate a full suite of endpoint protections

Identity Provider
Sufficient budget allocated to enable proper identity and access management

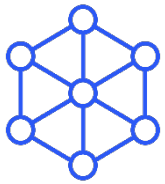
Pervasive MFA
Sufficient budget allocated to implement and operate a widely deployed MFA solution

Key Insights

- **Increase red team capability**
- **Increase security touchpoint with board of directors**
- **Embed security in business units**

Appendix

VisibleRisk Values

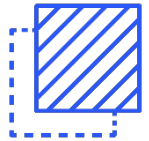


Holistic

We collect, analyze, and validate relevant external and internal data across multiple security and business dimensions.

Business-focused

We translate cyber risk by framing it in financial terms and providing a meaningful peer benchmark.



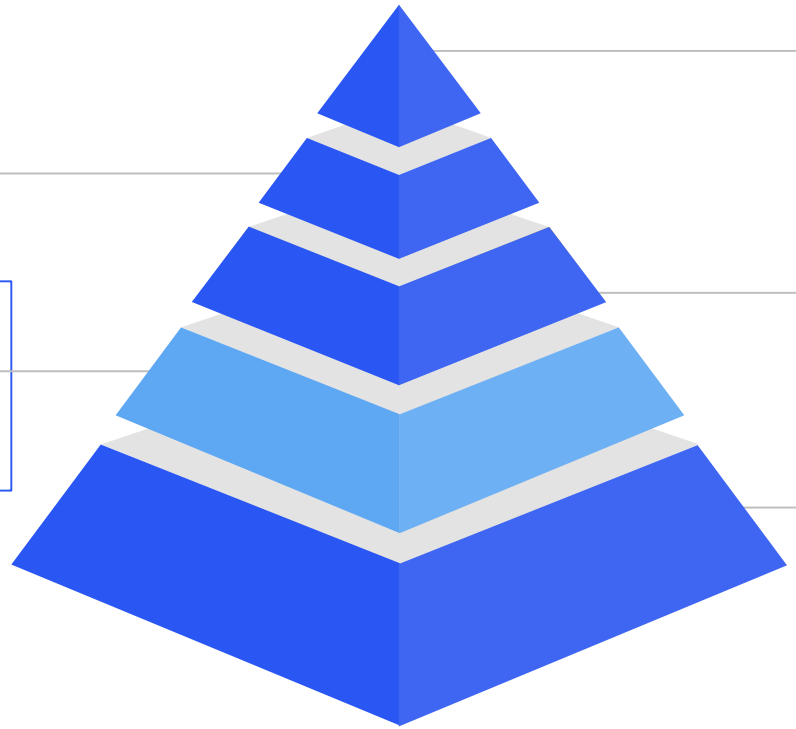
Transparent

We provide complete visibility into our ratings methodology. Focusing on assessment, and not remediation, maintains our integrity and independence.

© 2021 Cyber Assessments, Inc. All Rights Reserved. Confidential - Not for Further Redistribution

Peer Group Analysis: Selected Tiers

Organizations will be compared to one or more of the following groupings of similar organizations. This is used to determine relative risk compared to an organization's peers.



1 Cohort

Organizations that look the most like the target organization, grouped by granular NAICS codes in the same geographical location and with very similar size.

2 Cluster

Selection of organizations grouped by granular NAICS codes, in the same geo location and slightly expanded size.

3 Region

Organizations that operate in the same macro NAICS group code in the same geographic region.

Data Disclosure, Fraud and Business Interruption

4 Sector

Organizations operating in the same macro NAICS group across the globe

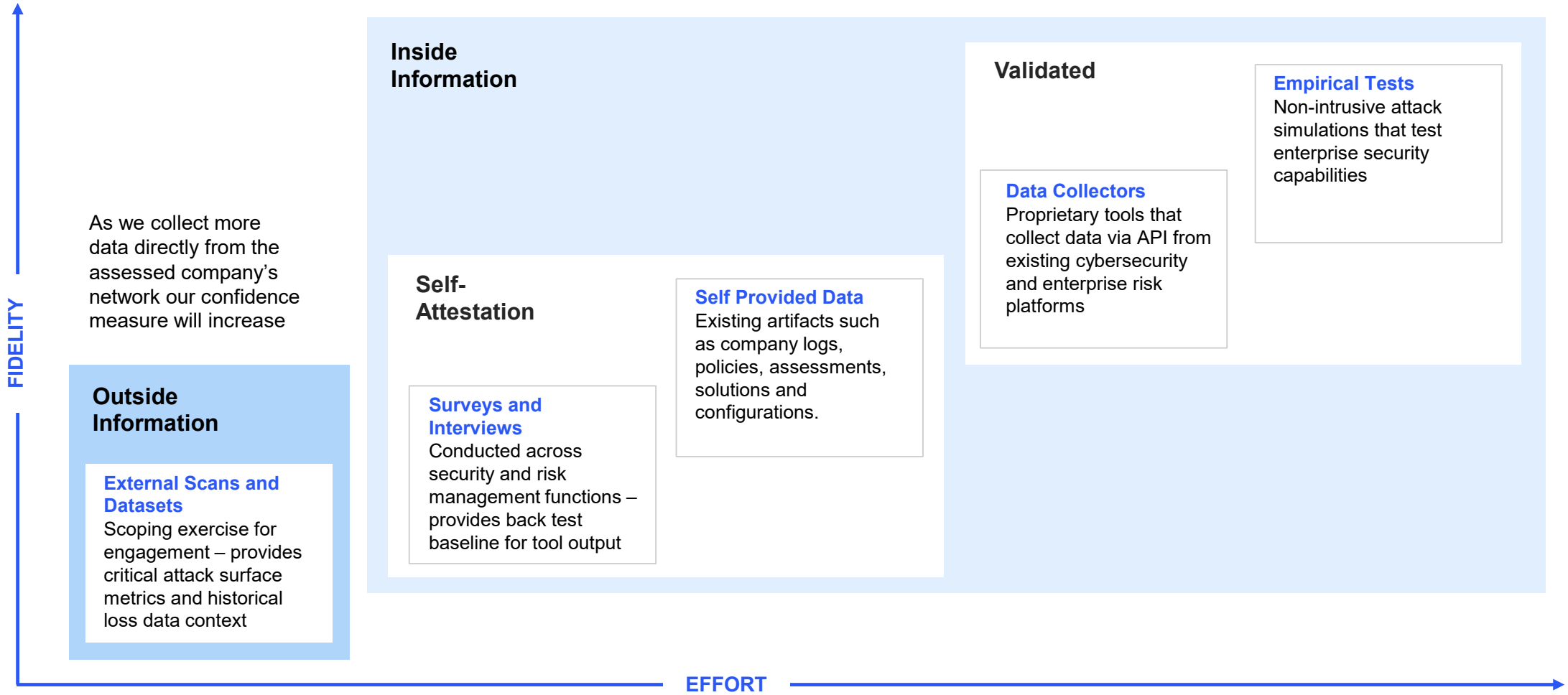
5 Global

All organizations matching 1) Industry classification, 2) Geography, and/or 3) organizations that have experienced an incident by type

© 2021 Cyber Assessments, Inc. All Rights Reserved. Confidential - Not for Further Redistribution

Data Collection - Fidelity vs. Effort

A holistic assessment requires a variety of data collection approaches and sources



© 2021 Cyber Assessments, Inc. All Rights Reserved. Confidential - Not for Further Redistribution

MOODY'S ANALYTICS

Quantitative Methods for Describing Emerging Threats

Cyber Events and Their Impact on Credit Risk

Select types of cyber events and sources of the resulting loss

Confidential Data Breach	System Failure	Malicious Activity Or Ransomware	Theft of IP or Technology
A Single Company Event Equifax 2017, Marriott 2018		Large-Scale Event SolarWinds 2020, WannaCry 2017, Net Petya 2016,	
Disruption of the company's core business	**Recovery costs**	**Legal costs**	**Damaged reputation**

Cyber Events and Their Impact on Credit Risk

Select types of cyber events and sources of the resulting loss

Confidential Data Breach	System Failure	Malicious Activity Or Ransomware	Theft of IP or Technology

A Single Company Event	Large-Scale Event
Equifax 2017, Marriott 2018	SolarWinds 2020, WannaCry 2017, Net Petya 2016,

Disruption of the company's core business	Recovery costs	Legal costs	Damaged reputation

How can cyber events change the creditworthiness of affected companies?

- Impact EDFs
- Contribute to rating reviews
- Lead to corporate bankruptcies

MOODY'S INVESTORS SERVICE December 2020

https://www.moodys.com/research/Moodys-places-SolarWinds-ratings-on-review-for-downgrade-following-announcement--PR_437591

Rating Action: Moody's places SolarWinds' ratings on review for downgrade following announcement of cyberattack

Forbes

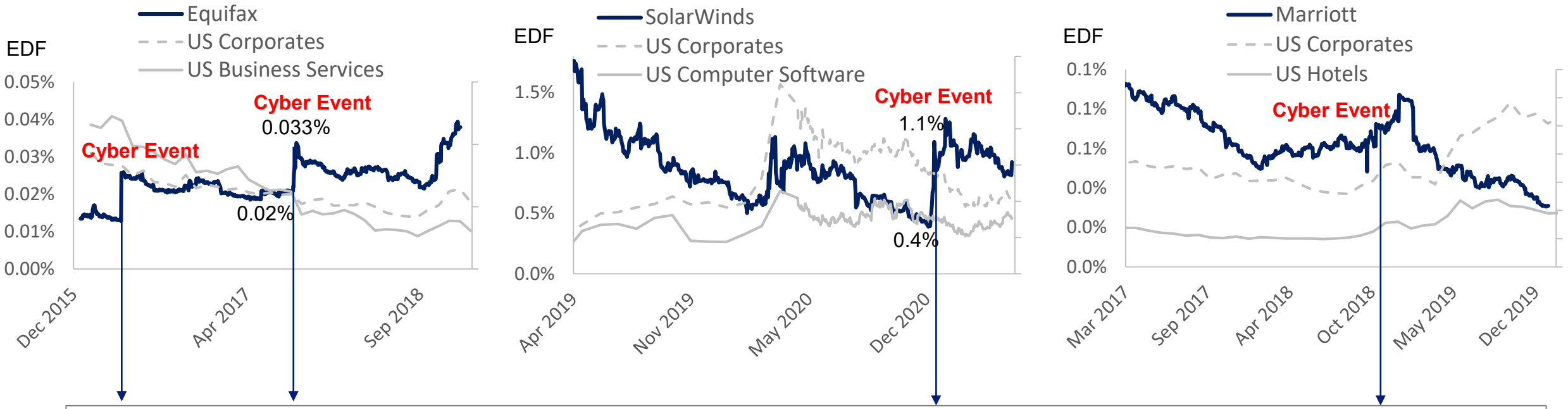
https://www.forbes.com/sites/taylorarmerding/2019/06/14/more-medical-mega-breaches-thanks-to-third-party-insecurity/?sh=7ce624216111

June 2019: Medical testing giants Quest Diagnostics and LabCorp announced…that personal and medical information of about 19.4 million patients had been compromised due to a breach of American Medical Collection Agency (AMCA), their billing collections vendor.

Retrieval-Masters Creditors Bureau Inc., which does business as AMCA, filed for Chapter 11 bankruptcy protection

When do Markets React to Cyber Events?

Using EDFs to quantify the real-time market reaction



What differentiates the magnitudes of impact?

Confidential data breach (retail customers) in a company's **core business**

Malicious activity: hackers used a SolarWinds **software update**, and its **core business**, to access the IT systems of hundreds of customers, ranging from corporations to government agencies

Confidential data breach (retail customers) in a hotel chain

Quantitative Modeling of a Cyber Event Impact

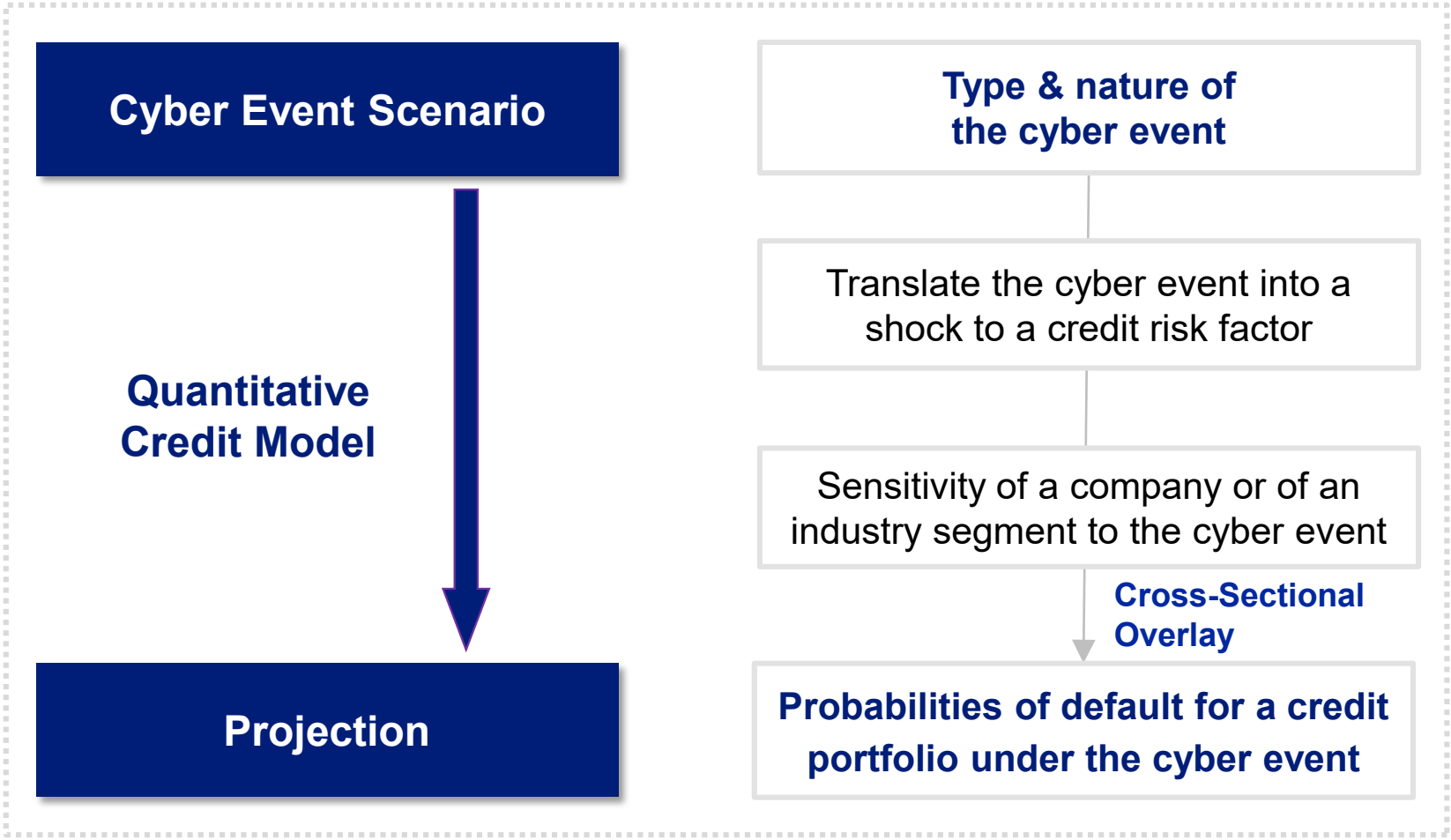
Challenges: Data sparsity & heterogeneous nature of cyber events

Cyber Event Scenario

Type & nature of the cyber event

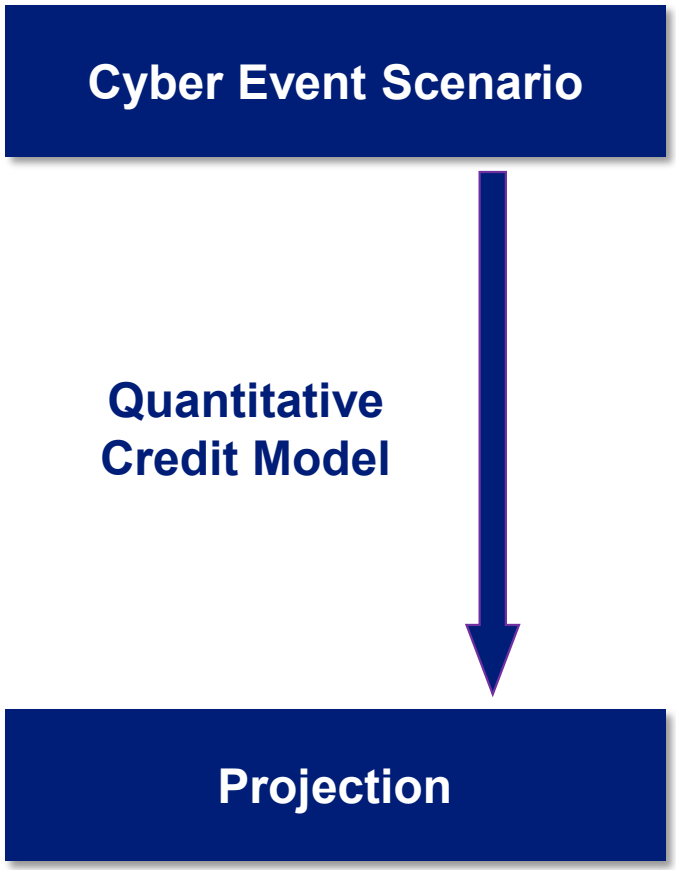
Quantitative Modeling of a Cyber Event Impact

Challenges: Data sparsity & heterogeneous nature of cyber events



Quantitative Modeling of a Cyber Event Impact

Challenges: Data sparsity & heterogeneous nature of cyber events



Type & nature of the cyber event

Translate the cyber event into a shock to a credit risk factor

Sensitivity of a company or of an industry segment to the cyber event

Cross-Sectional Overlay

Probabilities of default for a credit portfolio under the cyber event

Data & Calibration

EDF / Asset Return Data

Accounting Approach – Losses Relative to Company Size

Other data: equity prices (used in academic literature), CDS, Rating Changes, Defaults

Alternative Data

Segment / company data – past incidents, surveys, fundamental analysis

Qualitative Assessment

Alternative Data for Cyber Risk

Searching for measures of segments' sensitivity to cyber events

Verizon Dataset of Cyber Incidents
32,000 Incidents Over 2020, Global Dataset.

Industry Segment For challenges of cross-industry comparisons, see the report	Number of Past Cyber Events		
	Web Application Compromised	Internal Errors	Crimeware Ransomware
Accommodation	18	15	34
Administrative	10	2	5
Construction	10	0	10
Education	65	62	179
Entertainment	30	22	35
Finance	152	128	63
Healthcare	140	163	192
Information	162	115	403
Manufacturing	107	47	393
Mining+Utilities	16	6	21
Other Services	39	20	15
Professional	139	63	135
Public	149	112	800
Real Estate	14	6	1
Retail	66	21	55
Transportation	22	15	24

Ponemon Survey (2017)
Annualized Cost of Cyber Crime, Global Sample, 254 organizations

Industry Segment For challenges of cross-industry comparisons, see the report	Cost per firm-year Million USD
Financial services	18
Utilities and energy	17
Aerospace and defense	14
Technology and software	13
Healthcare	12
Services	11
Industrial/manufacturing	10
Retail	9
Public sector	8
Transportation	7
Consumer products	7
Communications	7
Life science	6
Education	5
Hospitality	5

MIS – Cyber Risk Heatmap (2019)
Qualitative Assessment

Sector	Vulnerability	Impact
Hospitals	HIGH	HIGH
Medical Devices	HIGH	MEDIUM
Banks	HIGH	HIGH
Basic Commodities	LOW	LOW
Consumer Products	MEDIUM	LOW
Lodging, Gaming	HIGH	MEDIUM
Manufacturing	HIGH	MEDIUM
Oil & Gas	LOW	MEDIUM

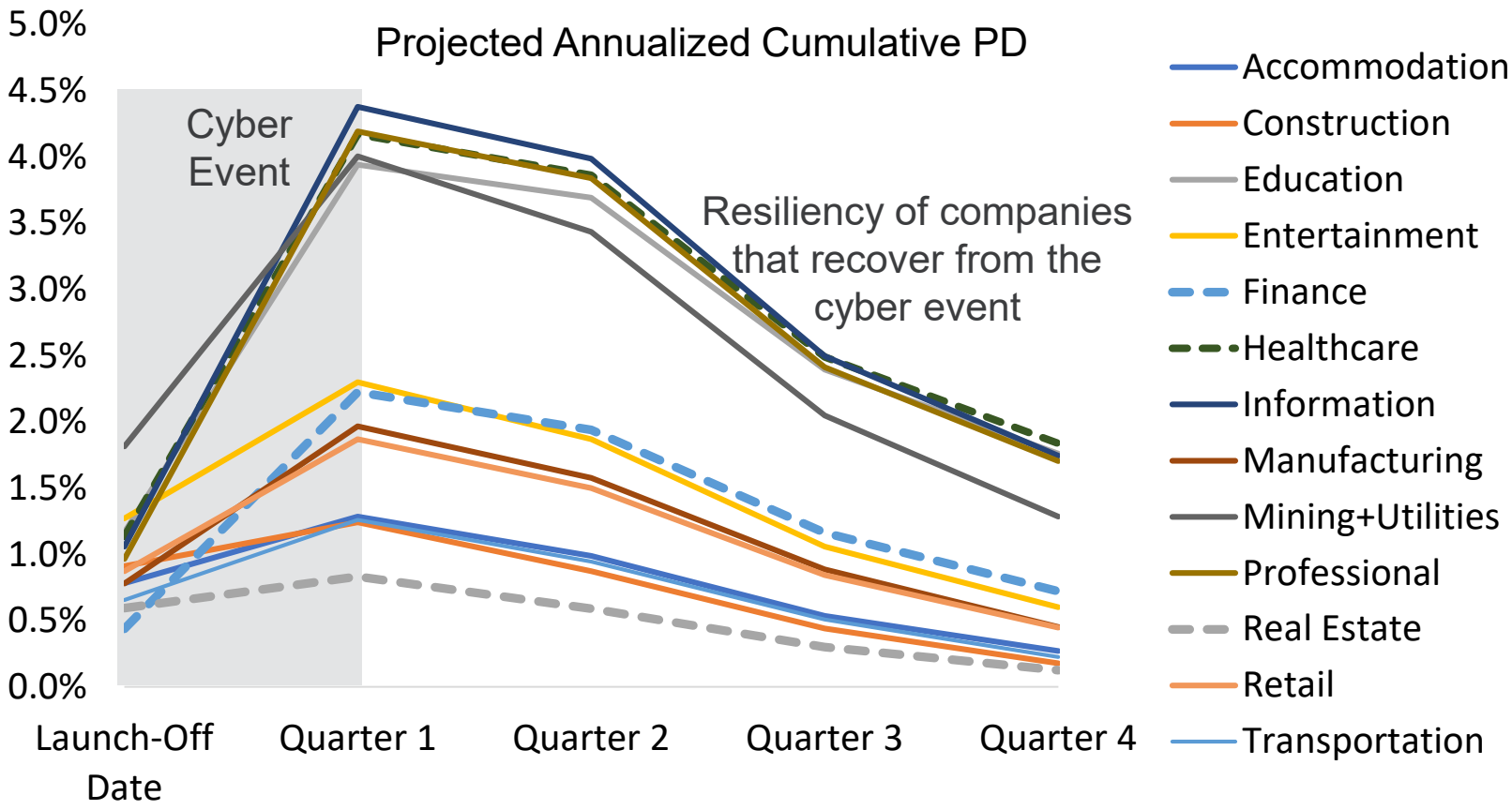
Constructing a segment-level score of sensitivity to cyber events

Quantifying a Cyber Scenario

Cross-sectional impact of a large-scale attack on credit

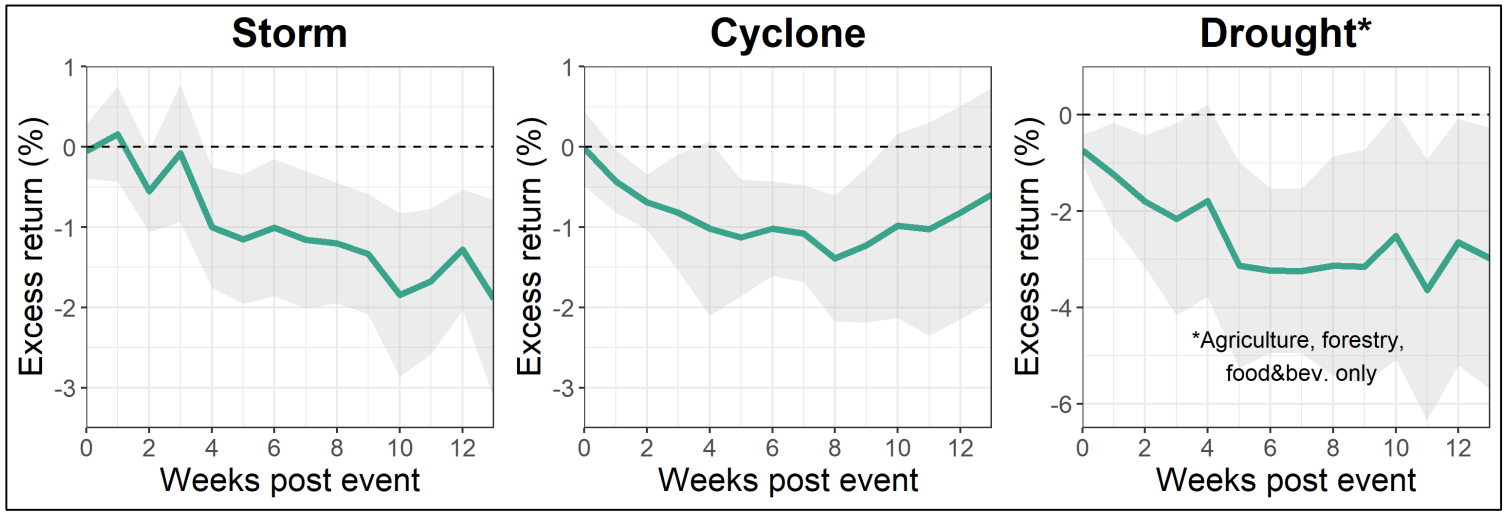
Cyber scenario calibrated to three times WannaCry or Not Petya ransomware attacks

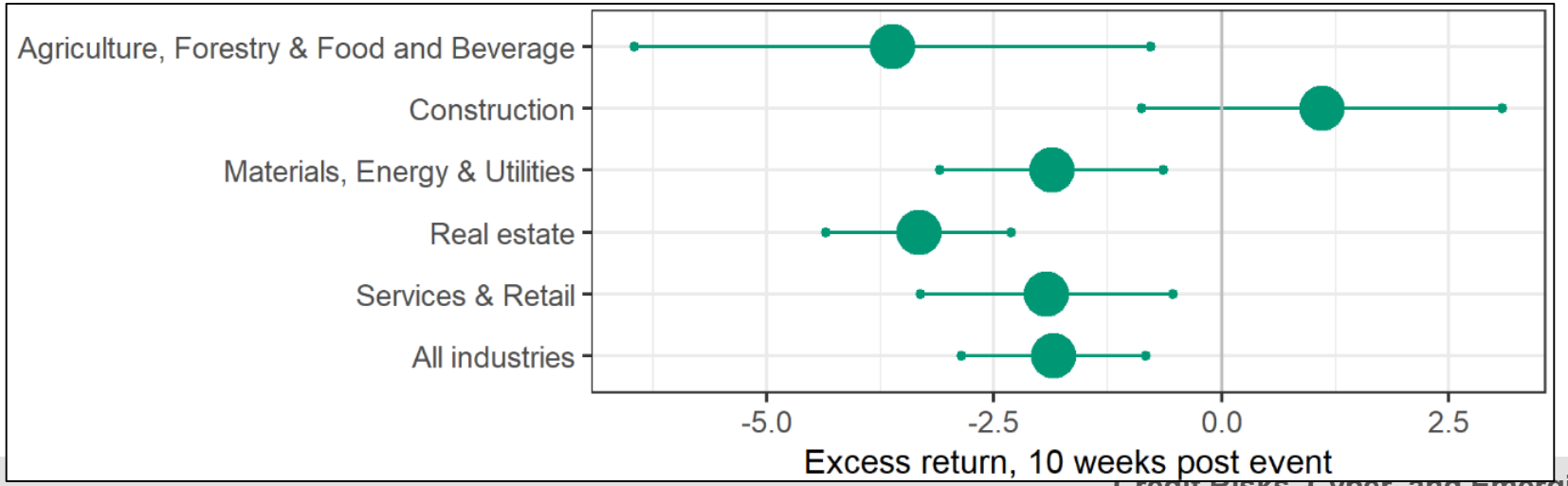
- The segments with the most pronounced PD shocks include **HEALTHCARE** and **FINANCE**
- On the other hand, segments such as **REAL ESTATE** see little impact



Quantifying Emerging Threats: Climate Hazards

Natural disasters and affected firms post-event excess asset returns

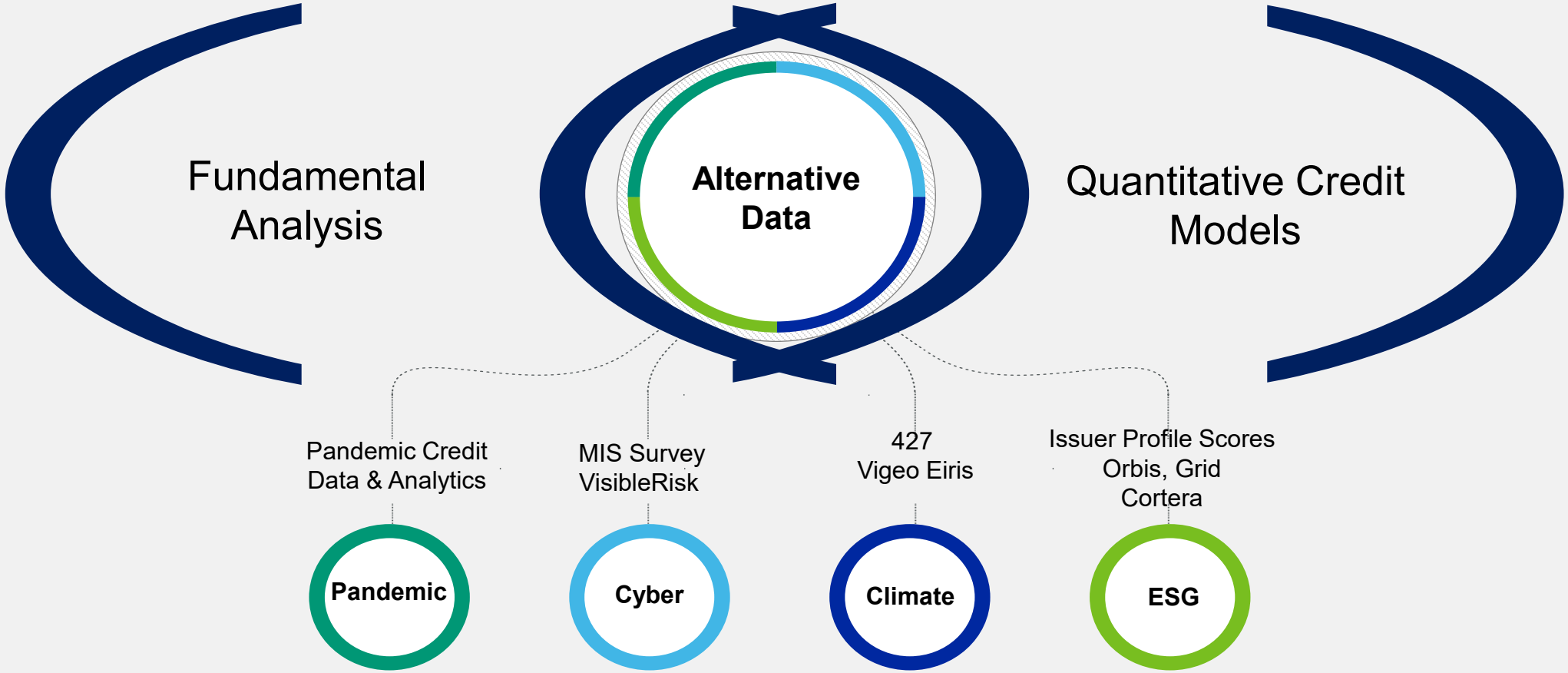




Ozkanoglu, O., Milonas, K., Zhao, S., Brizhatyuk, D., "An Empirical Assessment of the Financial Impacts of Climate-related Hazard Events" Moody's Analytics Research Paper, December 2020.

Credit Assessments and Emerging Threats

By their nature require articulation using alternative data



"if you've seen one pandemic, you've seen … one pandemic." Adam Kucharski

Q & A


MOODY'S
Better decisions
moodys.com

© 2021 Moody's Corporation, Moody's Investors Service, Inc., Moody's Analytics, Inc. and/or their licensors and affiliates (collectively, "MOODY'S"). All rights reserved.

CREDIT RATINGS ISSUED BY MOODY'S CREDIT RATINGS AFFILIATES ARE THEIR CURRENT OPINIONS OF THE RELATIVE FUTURE CREDIT RISK OF ENTITIES, CREDIT COMMITMENTS, OR DEBT OR DEBT-LIKE SECURITIES, AND MATERIALS, PRODUCTS, SERVICES AND INFORMATION PUBLISHED BY MOODY'S (COLLECTIVELY, "PUBLICATIONS") MAY INCLUDE SUCH CURRENT OPINIONS. MOODY'S DEFINES CREDIT RISK AS THE RISK THAT AN ENTITY MAY NOT MEET ITS CONTRACTUAL FINANCIAL OBLIGATIONS AS THEY COME DUE AND ANY ESTIMATED FINANCIAL LOSS IN THE EVENT OF DEFAULT OR IMPAIRMENT. SEE APPLICABLE MOODY'S RATING SYMBOLS AND DEFINITIONS PUBLICATION FOR INFORMATION ON THE TYPES OF CONTRACTUAL FINANCIAL OBLIGATIONS ADDRESSED BY MOODY'S CREDIT RATINGS. CREDIT RATINGS DO NOT ADDRESS ANY OTHER RISK, INCLUDING BUT NOT LIMITED TO: LIQUIDITY RISK, MARKET VALUE RISK, OR PRICE VOLATILITY. CREDIT RATINGS, NON-CREDIT ASSESSMENTS ("ASSESSMENTS"), AND OTHER OPINIONS INCLUDED IN MOODY'S PUBLICATIONS ARE NOT STATEMENTS OF CURRENT OR HISTORICAL FACT. MOODY'S PUBLICATIONS MAY ALSO INCLUDE QUANTITATIVE MODEL-BASED ESTIMATES OF CREDIT RISK AND RELATED OPINIONS OR COMMENTARY PUBLISHED BY MOODY'S ANALYTICS, INC. AND/OR ITS AFFILIATES. MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND PUBLICATIONS DO NOT CONSTITUTE OR PROVIDE INVESTMENT OR FINANCIAL ADVICE, AND MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND PUBLICATIONS ARE NOT AND DO NOT PROVIDE RECOMMENDATIONS TO PURCHASE, SELL, OR HOLD PARTICULAR SECURITIES. MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND PUBLICATIONS DO NOT COMMENT ON THE SUITABILITY OF AN INVESTMENT FOR ANY PARTICULAR INVESTOR. MOODY'S ISSUES ITS CREDIT RATINGS, ASSESSMENTS AND OTHER OPINIONS AND PUBLISHES ITS PUBLICATIONS WITH THE EXPECTATION AND UNDERSTANDING THAT EACH INVESTOR WILL, WITH DUE CARE, MAKE ITS OWN STUDY AND EVALUATION OF EACH SECURITY THAT IS UNDER CONSIDERATION FOR PURCHASE, HOLDING, OR SALE.

MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS, AND PUBLICATIONS ARE NOT INTENDED FOR USE BY RETAIL INVESTORS AND IT WOULD BE RECKLESS AND INAPPROPRIATE FOR RETAIL INVESTORS TO USE MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS OR PUBLICATIONS WHEN MAKING AN INVESTMENT DECISION. IF IN DOUBT YOU SHOULD CONTACT YOUR FINANCIAL OR OTHER PROFESSIONAL ADVISER.

ALL INFORMATION CONTAINED HEREIN IS PROTECTED BY LAW, INCLUDING BUT NOT LIMITED TO, COPYRIGHT LAW, AND NONE OF SUCH INFORMATION MAY BE COPIED OR OTHERWISE REPRODUCED, REPACKAGED, FURTHER TRANSMITTED, TRANSFERRED, DISSEMINATED, REDISTRIBUTED OR RESOLD, OR STORED FOR SUBSEQUENT USE FOR ANY SUCH PURPOSE, IN WHOLE OR IN PART, IN ANY FORM OR MANNER OR BY ANY MEANS WHATSOEVER, BY ANY PERSON WITHOUT MOODY'S PRIOR WRITTEN CONSENT.

MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND PUBLICATIONS ARE NOT INTENDED FOR USE BY ANY PERSON AS A BENCHMARK AS THAT TERM IS DEFINED FOR REGULATORY PURPOSES AND MUST NOT BE USED IN ANY WAY THAT COULD RESULT IN THEM BEING CONSIDERED A BENCHMARK.

All information contained herein is obtained by MOODY'S from sources believed by it to be accurate and reliable. Because of the possibility of human or mechanical error as well as other factors, however, all information contained herein is provided "AS IS" without warranty of any kind. MOODY'S adopts all necessary measures so that the information it uses in assigning a credit rating is of sufficient quality and from sources MOODY'S considers to be reliable including, when appropriate, independent third-party sources. However, MOODY'S is not an auditor and cannot in every instance independently verify or validate information received in the rating process or in preparing its Publications.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability to any person or entity for any indirect, special, consequential, or incidental losses or damages whatsoever arising from or in connection with the information contained herein or the use of or inability to use any such information, even if MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers is advised in advance of the possibility of such losses or damages, including but not limited to: (a) any loss of present or prospective profits or (b) any loss or damage arising where the relevant financial instrument is not the subject of a particular credit rating assigned by MOODY'S.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability for any direct or compensatory losses or damages caused to any person or entity, including but not limited to by any negligence (but excluding fraud, willful misconduct or any other type of liability that, for the avoidance of doubt, by law cannot be excluded) on the part of, or any contingency within or beyond the control of, MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers, arising from or in connection with the information contained herein or the use of or inability to use any such information.

NO WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, TIMELINESS, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OF ANY CREDIT RATING, ASSESSMENT, OTHER OPINION OR INFORMATION IS GIVEN OR MADE BY MOODY'S IN ANY FORM OR MANNER WHATSOEVER.

Moody's Investors Service, Inc., a wholly-owned credit rating agency subsidiary of Moody's Corporation ("MCO"), hereby discloses that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by Moody's Investors Service, Inc. have, prior to assignment of any credit rating, agreed to pay to Moody's Investors Service, Inc. for credit ratings opinions and services rendered by it fees ranging from $1,000 to approximately $5,000,000. MCO and Moody's Investors Service also maintain policies and procedures to address the independence of Moody's Investors Service credit ratings and credit rating processes. Information regarding certain affiliations that may exist between directors of MCO and rated entities, and between entities who hold credit ratings from Moody's Investors Service and have also publicly reported to the SEC an ownership interest in MCO of more than 5%, is posted annually at www.moodys.com under the heading "Investor Relations — Corporate Governance — Director and Shareholder Affiliation Policy."

Additional terms for Australia only: Any publication into Australia of this document is pursuant to the Australian Financial Services License of MOODY'S affiliate, Moody's Investors Service Pty Limited ABN 61 003 399 657AFSL 336969 and/or Moody's Analytics Australia Pty Ltd ABN 94 105 136 972 AFSL 383569 (as applicable). This document is intended to be provided only to "wholesale clients" within the meaning of section 761G of the Corporations Act 2001. By continuing to access this document from within Australia, you represent to MOODY'S that you are, or are accessing the document as a representative of, a "wholesale client" and that neither you nor the entity you represent will directly or indirectly disseminate this document or its contents to "retail clients" within the meaning of section 761G of the Corporations Act 2001. MOODY'S credit rating is an opinion as to the creditworthiness of a debt obligation of the issuer, not on the equity securities of the issuer or any form of security that is available to retail investors.

Additional terms for Japan only: Moody's Japan K.K. ("MJKK") is a wholly-owned credit rating agency subsidiary of Moody's Group Japan G.K., which is wholly-owned by Moody's Overseas Holdings Inc., a wholly-owned subsidiary of MCO. Moody's SF Japan K.K. ("MSFJ") is a wholly-owned credit rating agency subsidiary of MJKK. MSFJ is not a Nationally Recognized Statistical Rating Organization ("NRSRO"). Therefore, credit ratings assigned by MSFJ are Non-NRSRO Credit Ratings. Non-NRSRO Credit Ratings are assigned by an entity that is not a NRSRO and, consequently, the rated obligation will not qualify for certain types of treatment under U.S. laws. MJKK and MSFJ are credit rating agencies registered with the Japan Financial Services Agency and their registration numbers are FSA Commissioner (Ratings) No. 2 and 3 respectively.

MJKK or MSFJ (as applicable) hereby disclose that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by MJKK or MSFJ (as applicable) have, prior to assignment of any credit rating, agreed to pay to MJKK or MSFJ (as applicable) for credit ratings opinions and services rendered by it fees ranging from JPY125,000 to approximately JPY550,000,000.

MJKK and MSFJ also maintain policies and procedures to address Japanese regulatory requirements.