

Cyber Risk In A New Era

Cyber Risk Analytics

October 23, 2020



S&P Global
Ratings

Cyber Risk In A New Era

Cyber Risk Analytics

Moderator

Simon Ashworth

Head of Analytics & Research – Insurance Ratings

S&P Global Ratings

simon.ashworth@spglobal.com

What to expect today

- 1 | Overview of how S&P Global Ratings embeds cyber risks in our analysis:
Governance and stakeholder trust as key themes
- 2 | Results from a quantitative study of historic cyber data breaches
- 3 | External insights provided by Erin Kenneally
Director of Cyber Risk Analytics, Guidewire-Cyence

Cyber Insights: Single Point Of Contact

<https://www.spglobal.com/ratings/en/research-insights/topics/cyber-risk-in-a-new-era>

S&P Global
Ratings

Ratings

Research & Insights

Sectors

Regulatory

Products & Benefits

Events



Cyber Risk in a New Era

The increasing frequency of cyber attacks and the potential for rapid deterioration in credit profiles after an attack are risk factors that are relevant for our rating assessments now.

Cyber

Sector

- Corporates
- Infrastructure & Utilities +
- Insurance +
- U.S. Public Finance

Content Type

- Article

COMMENTS — Oct 19, 2020

Cyber Risk In A New Era: Disruptions And Distractions Increase Challenges For U.S. Public Finance Issuers

COMMENTS — Sep 17, 2020

Cyber Risk In A New Era: Remedy First, Prevent Second

COMMENTS — Sep 2, 2020 — Canada, APAC, Latin America, APAC, EMEA, United States of America

Cyber Risk In A New Era: Insurers Can Be Part Of The Solution

S&P Global
Ratings

Cyber Risk In A New Era

Cyber Risk Analytics

Erin Kenneally
Director of Cyber Risk Analytics
Guidewire-Cyence



Cyber Risk Insights

Lead with Data.
Follow the Tech.

Erin Kenneally | Director Cyber Risk Analytics | Guidewire-Cyence



Human Element

- Phishing
- BEC
- Scams



Web & Browser-based Attacks

- Drive-by Download
- Malvertising
- Exploit kits



Internet-Exposed Assets

- Password re-use
- Weak credentials



Vulnerabilities, Misconfigurations

- Supply chain attacks



Active Network Attacks

- Privilege Misuse
- Misinformation
- Fileless attacks



\$1
Hacking Kits



19B
Dark Web sites



\$6T/yr (by 2021)
Cyber Crime Cost

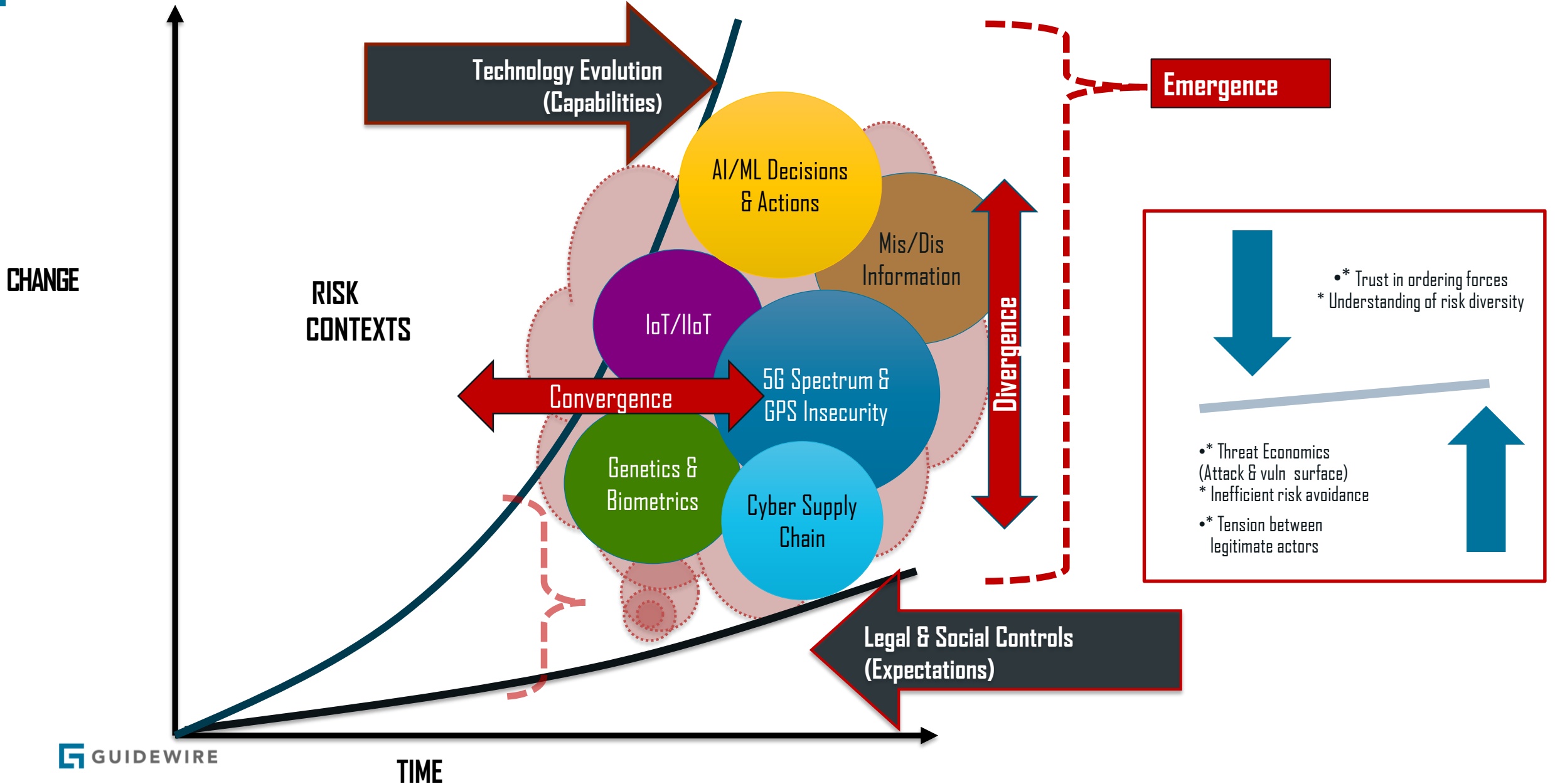


50% more valuable
Health/Medical Data

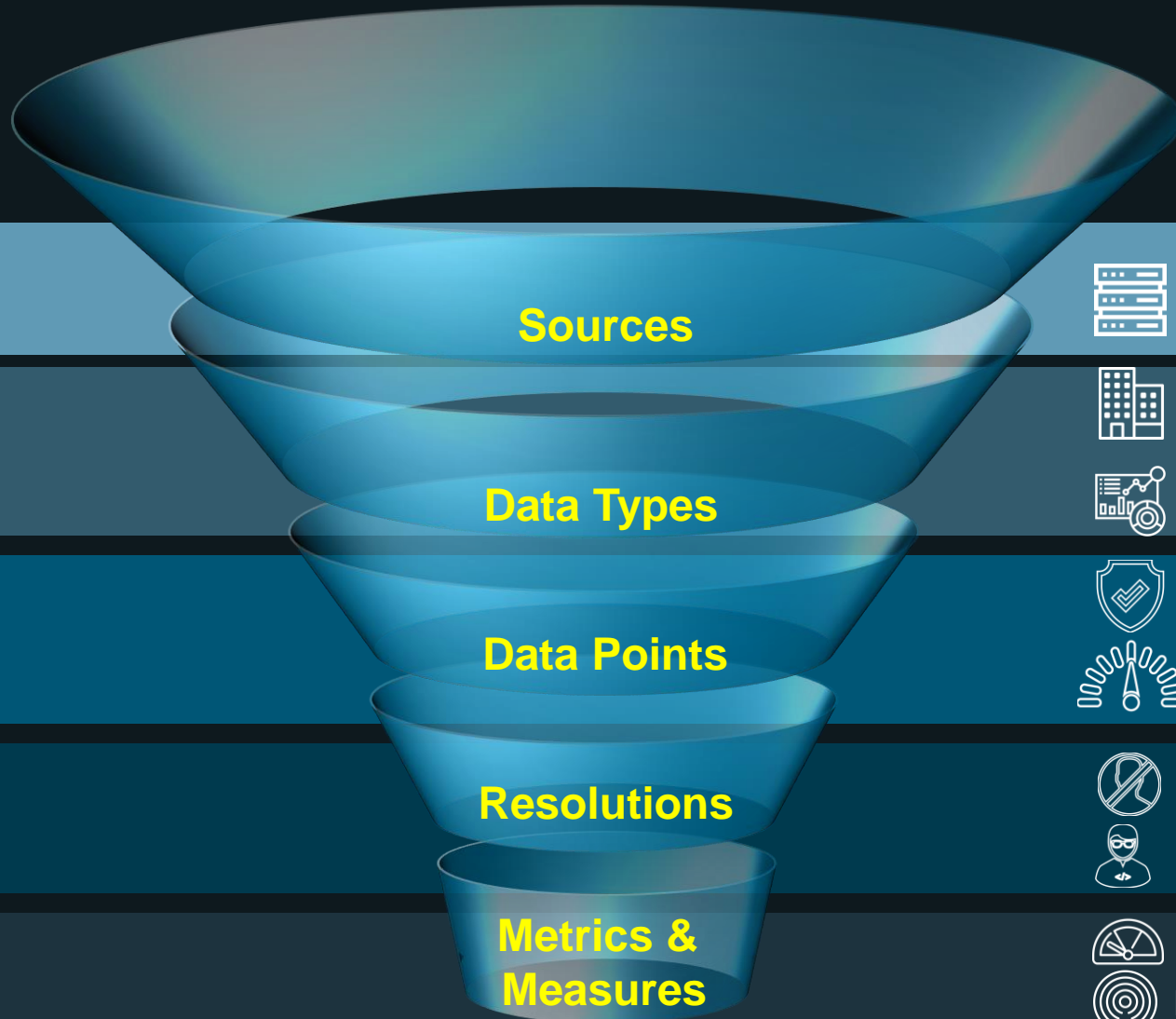





























\$1T
Cyber Security Spending

Cyber Risk Canvas & Crystal Ball

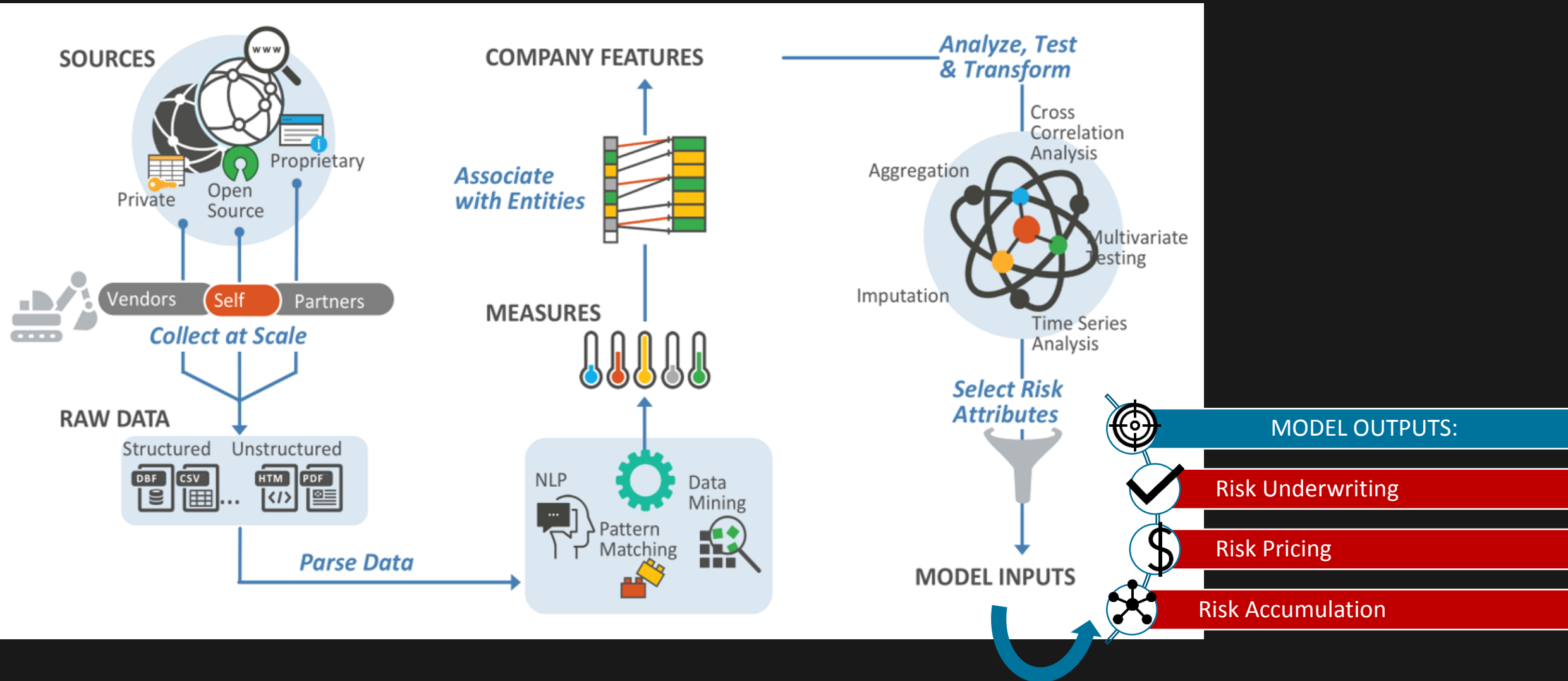


Cyber Risk Sensemaking



 Proprietary	 Private	 Open Source
 Firmographics	 Outside-In	 Inside-Out
 Threats	 Process & Policy	 Incidents
 SPF Configurations	 Cloud Service Providers	 DNS Leakage
 Malicious Indicators	 Patching Cadence	 1000+
 Bad Activity	 Infrastructure	 Perimeter Posture
 Risky Tech	 External Presence	 Cyber Supply Chain
 Risk Rating	 Peer Comparison	 Accumulation Models
 Exposure Signals	 ←Company/Portfolio→	 Loss Models

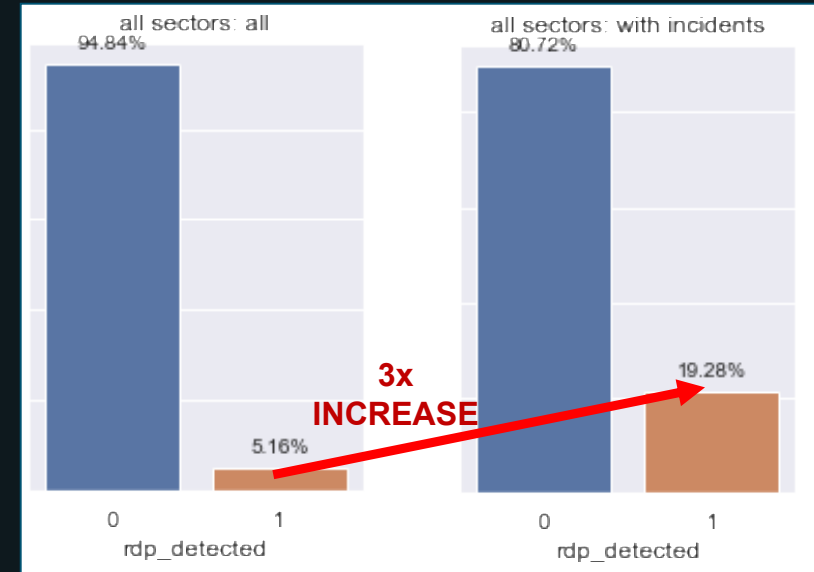
Cyber Risk Sensemaking Under the Hood



Data to Assess Risk: Exposure Signals & Perils



- How to identify if a company is at a higher risk of Ransomware attack?
- **Exposure Signal:** Proven correlation between having Remote Desktop Protocol (RDP) exposed & Ransomware incidents
- The likelihood of a company having a Ransomware incident increases by over 3x if they've had RDP exposed



45x	22x	22x	20x	7x	4x	3-4x
Targeted Darkweb Chatter	Leaked User Accounts	High Risk Rating	Compromised User Passwords	DNS Leakage	Spam Activity	Email Misconfig

Data to Select Risk: Exposure Signals Combined



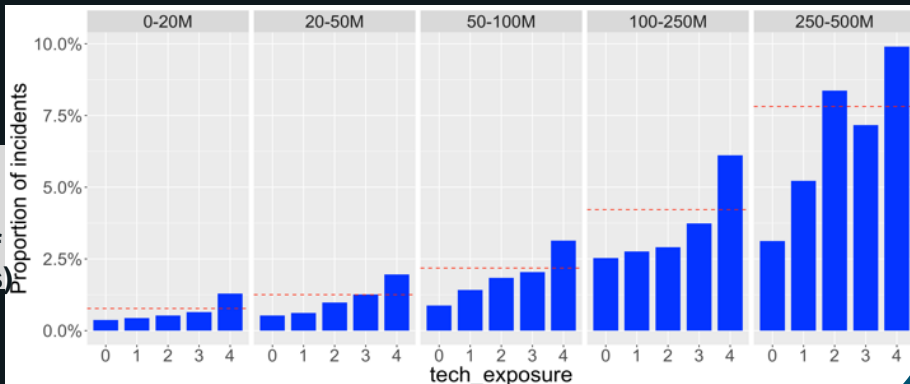
Tech Exposure

Category	% of detected companies	# of incidents (compared to average)
Printers	0.4%	6x
ICS devices	1.0%	4x
Communication	1.3%	3x
Payment	13%	2.5x
Databases	32%	1.5x

Combined and normalized by company size (# of domains)

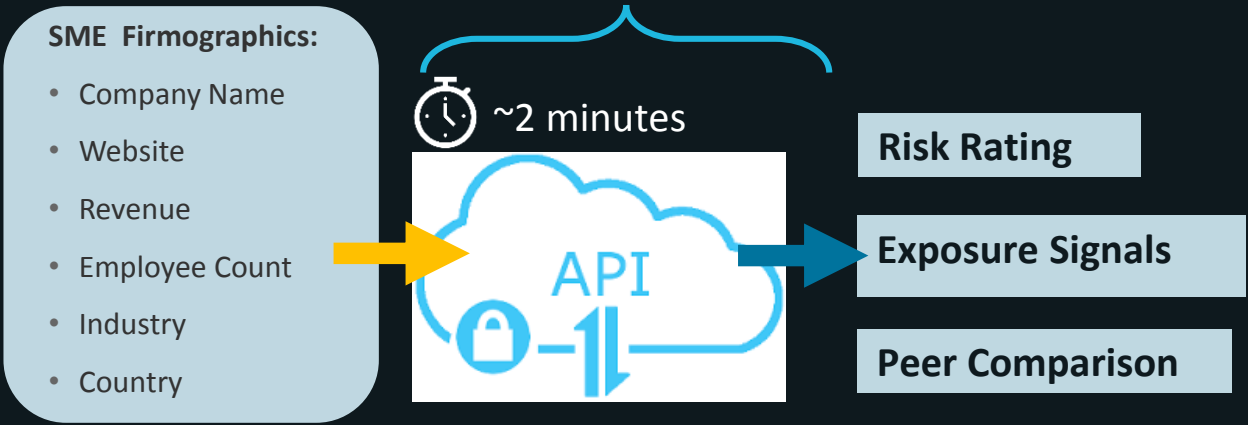
Signal

Baseline (avg. # of incidents)



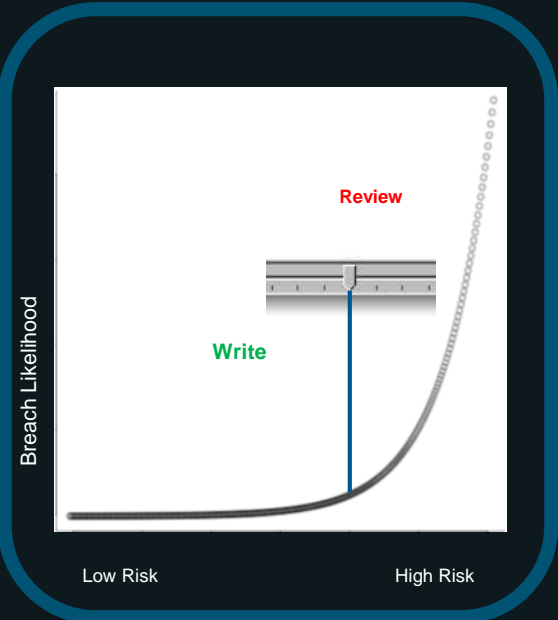
Data to Price Risk: Quick Quotes & Loss Modeling

Price Risks Quickly

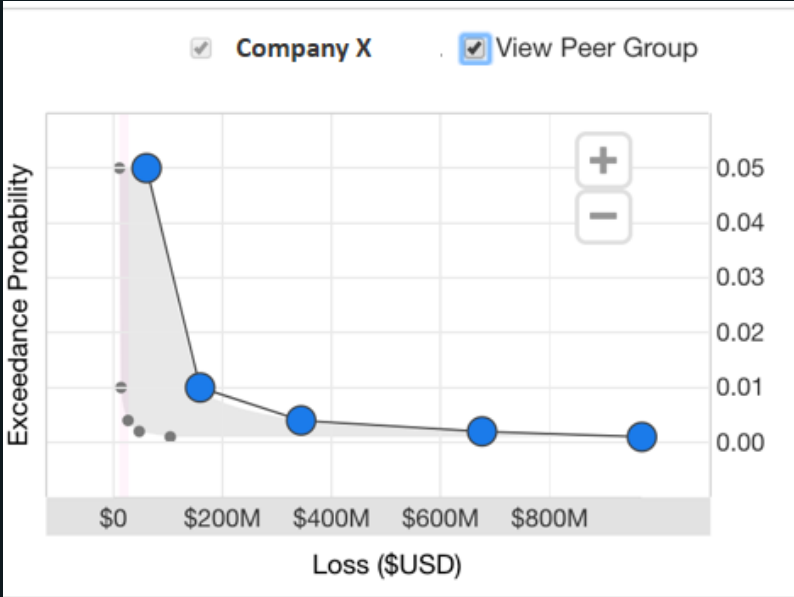


Inputs

Outputs



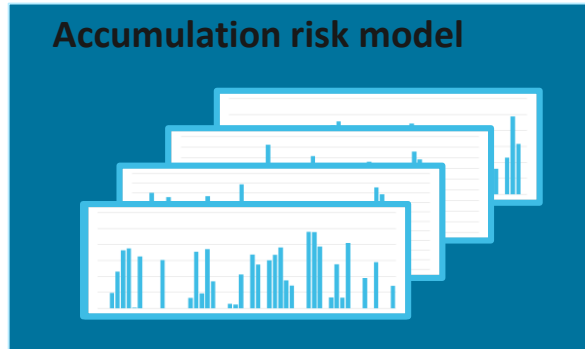
Price Risks by Coverage



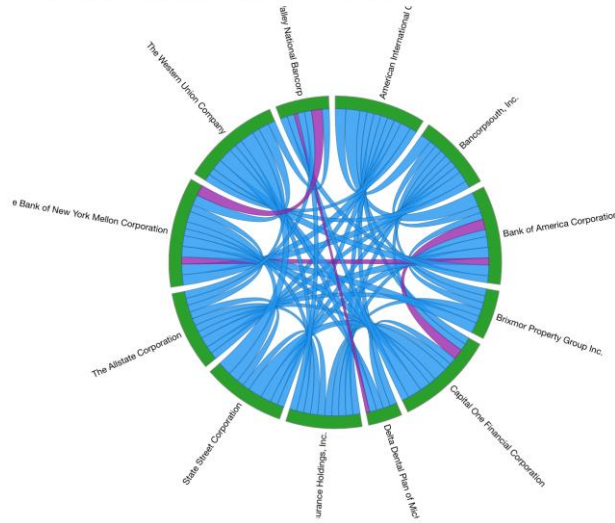
Exceedance probability curve

Average annual loss [?]	\$17,142,038
Liability	\$540,995
First party breach costs	\$7,230,164
Business interruption	\$3,898,426
Contingent business interruption	\$5,472,454

Data to Understand Risk Accumulation



Visualizations – Overlays
 For your selected path(s) of aggregation, we tie together companies in your portfolio that share multiple low frequency features or attributes. The most common paths are excluded to better illustrate the less obvious paths of aggregate risk in your portfolio.



Paths: All - None

- Service providers
- Software
- Payment processors
- Auditors
- Hide unconnected companies
- Financial Services

Order:
 Industry

Service provider outage

- Types**
- Cloud
 - ISP
 - CDN
 - DNS

- Coverages**
- Contingent business interruption

Count

- 5,000

Example

- Rackspace Texas cloud provider

Zero-day vulns

- Types**
- Databases
 - Operating systems
 - Web apps
 - .. & 5 others

- Coverages**
- Liability
 - Data breach
 - Business interruption

Count

- 400

Example

- Windows OS

Payment processor outage

- Types**
- Payment processor

- Coverages**
- Contingent business interruption

Count

- 50

Example

- Paypal



Navigate what's next.

Legal Notice

Guidewire Proprietary & Confidential – DO NOT DISTRIBUTE
©2020 Guidewire Software, Inc.

For information about Guidewire's trademarks, visit <https://guidewire.com/legal-notices>

Cyber Risk In A New Era

Cyber Risk Analytics – Cyber In Ratings



Cyber Risk In A New Era

Cyber Risk Analytics

Methodologies

Nik Khakee

Managing Director

S&P Global Ratings

nik.khakee@spglobal.com

Overview | **Cyber In Ratings Analysis - FAQs**

Is considering cyber risk a new development at S&P Global Ratings?

No. We published our first substantive commentaries on the emerging importance of Cyber Risk to issuer creditworthiness as far back as June 2015 in articles such as:

- Corporate ratings: Cyber Risk And Corporate Credit (6/9/2015)
- Financial Institutions: U.S. Financial Services Credit Ratings Are Resilient To Cyber US Public Finance Security--For Now (6/9/2015)
- USPF, Corporate: Should Cyber Threats Scare You? Public Finance, Utilities, And Infrastructure Roundtable Asks (12/6/2018)

And more recently, we identified key aspects of issuer Governance we consider when considering cyber risk management in articles such as:

- US Public Finance: Cyber Risk Management For U.S. Municipal Utilities Should Be Routine And Requires Vigilance And Flexibility (2/3/2020)

Overview | Cyber In Ratings Analysis - FAQs

Where would or could cyber risk appear in S&P Global Ratings analysis?

We consider cyber risk through the lens of ESG.

While sometimes resulting from **Environmental** considerations, and sometimes due to **Social** considerations, we view cyber risk as first and foremost a **Governance** consideration in our corporate, insurance, financial institutions, infrastructure and government ratings analysis.

- Because cyber risk is typically reflective of the susceptibility of an issuer to a successful cyber-attack and of the motivation of those outside the company to executing a cyber-attack, we consider the issuer's focus on and commitment to cyber-defense and what we sometimes call 'good cyber-hygiene'.
- While each team considers issuer cyber risk management from its sector specific focus, our questions and issuer management practice often reflects aspects of the **NIST** (National Institute of Standards and Technology) Framework Core:
 - Identify
 - Protect
 - Detect
 - Respond
 - Recover

Overview | Cyber In Ratings Analysis - FAQs

Where else would or could cyber risk appear in S&P Global Ratings analysis?

In our corporate, insurance, financial institutions, infrastructure and government ratings analysis, cyber risk could appear in one or more of the following:

- Perceived or real risk of potential successful cyber-attack may weaken
 - Business or Enterprise Position or Risk due to weakened client confidence and competitive position
 - Funding due to weakened confidence of capital providers
- Successful attacks may cause swings in:
 - Capital, Cash Flow and/or Earnings
 - Liquidity

We view cyber risk as similar to **Event Risk**. Cyber-attacks, like any event risk, can pressure liquidity and operational balance, and can further create contingent liabilities.

We do not model cyber risk events as a base case, but we actively assess operational risks and controls. We may consider the potential financial impact of cyber-attack, of additional costs and losses after a cyber-attack, and we do have access to the Guidewire platform's for additional insight.

Cyber Risk In A New Era

Cyber Risk Analytics

U.S. Public Finance

Geoff Buswick

Managing Director – State Governments

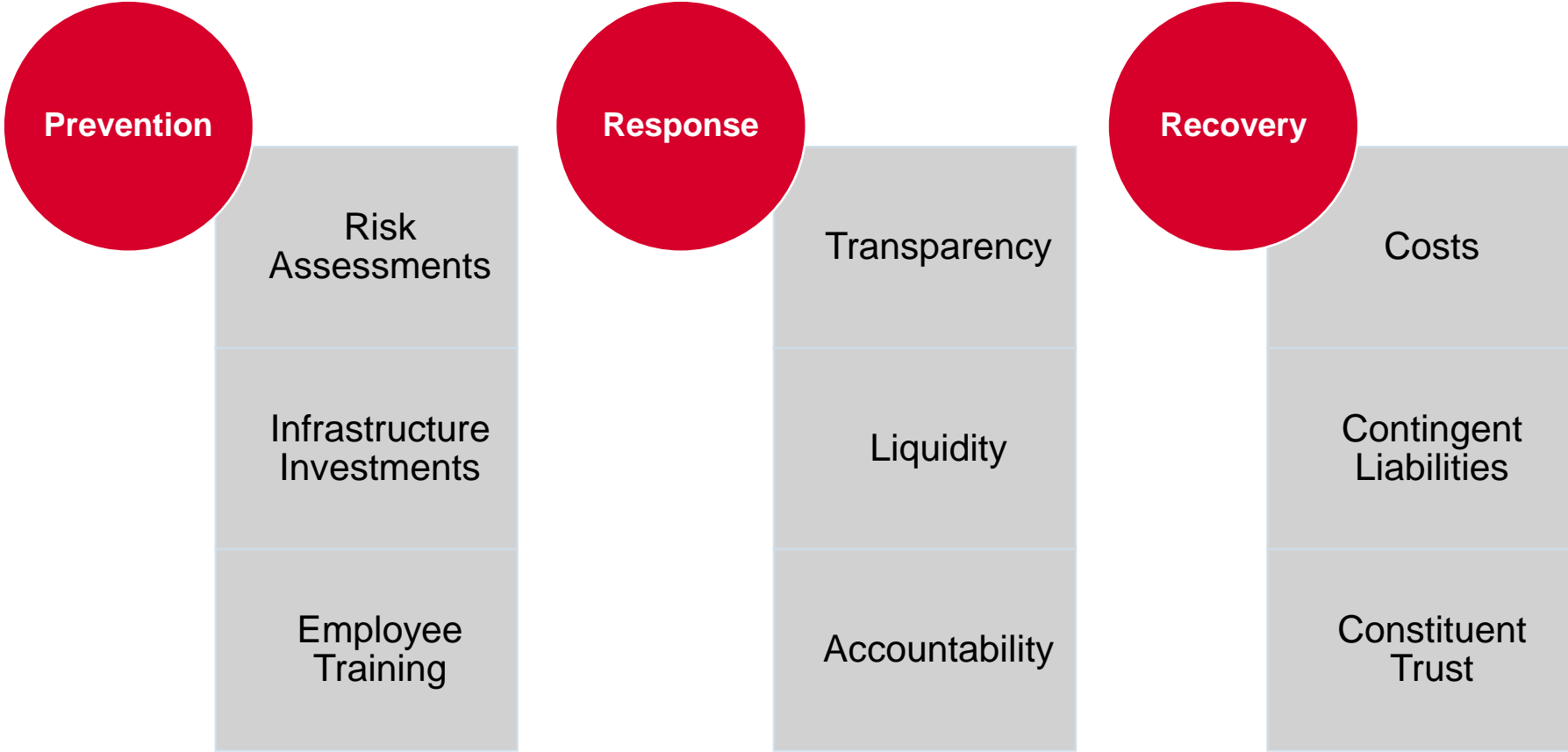
S&P Global Ratings

geoffrey.buswick@spglobal.com

USPF | Immediate Liquidity Risk – Long-term Credit Risk

- Cyber related risks are likely to become greater in public finance before they are mitigated
- The very nature of public finance attracts criminals
- Revenue declines driven by the pandemic make it hard for governments to counter the cyber threat
- Professionalism of the cybercriminals is giving the attackers a current advantage
 - Additionally periods of disruption are times when attacks could occur
- Although each cyberattack is an event that could affect credit, **the recurring nature and impact on public trust is potentially a greater risk to public finance**

USPF | Immediate Liquidity Risk – Long-term Credit Risk



USPF | Cyber Risk As An ESG Consideration

Environmental, social, and governance (ESG) factors are key features embedded in credit analysis. Environmental and social events can be drivers for cybercriminal actions; however, in U.S. public finance, we view cyber risk mitigation mainly as a governance opportunity.



E – Cybercriminals use environmental disasters as cover for attacks. They expect an entity's focus will be elsewhere or it will pay quickly to remove the cyber risk. Emergency planning for both natural disasters and cyberattacks can help maintain credit quality.



S – In some cases, public finance issuers make decisions to protect their entities that could elicit an emotional response leading to hacktivist actions. These attacks could have the long-term effect of causing reputational damage, should the attacks be seen as avoidable. Hacktivist attacks are not typically motivated by money, but simply aim to send a message.



G - **We believe the inability to minimize cyber vulnerability illustrates poor risk management and failure to develop a long-term strategy for protective measures. This could lead to headline risk and negatively affect credit quality. Conversely, a proactive approach to planning and prevention, and maintaining good cyber hygiene can support our view of strong governance.**

Source: S&P Global Ratings.
Copyright © 2020 by Standard & Poor's Financial Services LLC. All rights reserved.

Cyber Risk In A New Era

Cyber Risk Analytics

Corporate Ratings

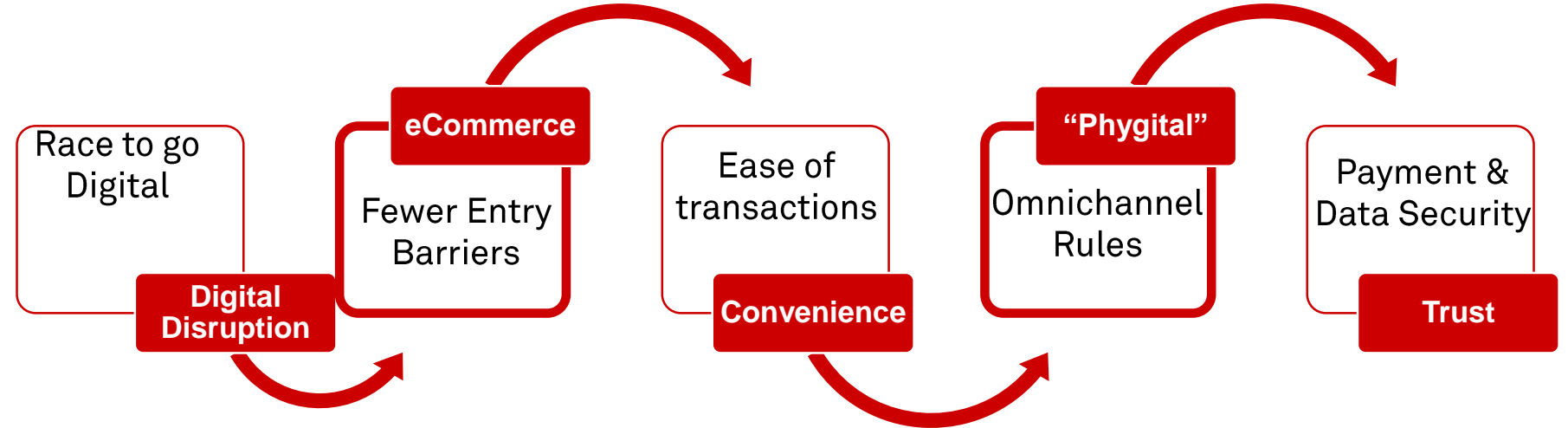
Raam Ratnam

Senior Director

S&P Global Ratings

raam.ratnam@spglobal.com

Corporates | Vital To Adopt A Holistic Approach In A Digital World



<ul style="list-style-type: none"> • Disparate and legacy systems • Processes not fully fit for purpose 	<ul style="list-style-type: none"> • Newer entrants • Brands equity - Trust amid choice 	<ul style="list-style-type: none"> • 24X7 Availability • Interconnected value chain, Automation & AI 	<ul style="list-style-type: none"> • Brick & mortar ops & digital function in sync • Outsourcing is inevitable 	<ul style="list-style-type: none"> • Fraud/data breach is costly • Loss of customer trust is often > Monetary fines
---------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------

Credit Impact

- **Business Risk:** Well managed and secure systems can drive Competitive advantage and Operating efficiency, while operations and profits can be significantly impacted in the event of a cyber incident/attack.
- **Financial Risk:** Ongoing need to invest (often when cash flows are pressured) is a challenge for smaller & leveraged companies; Loss of earnings, fines and remediation opex and capex can impact financial position and liquidity.
- **Management and Governance:** Cyber risk resilience and incident management speaks to effectiveness of risk management, internal controls, operating efficiency & communication of messages.

Cyber Risk In A New Era

Cyber Risk Analytics

Insurance Ratings

Manuel Adam

Associate

S&P Global Ratings

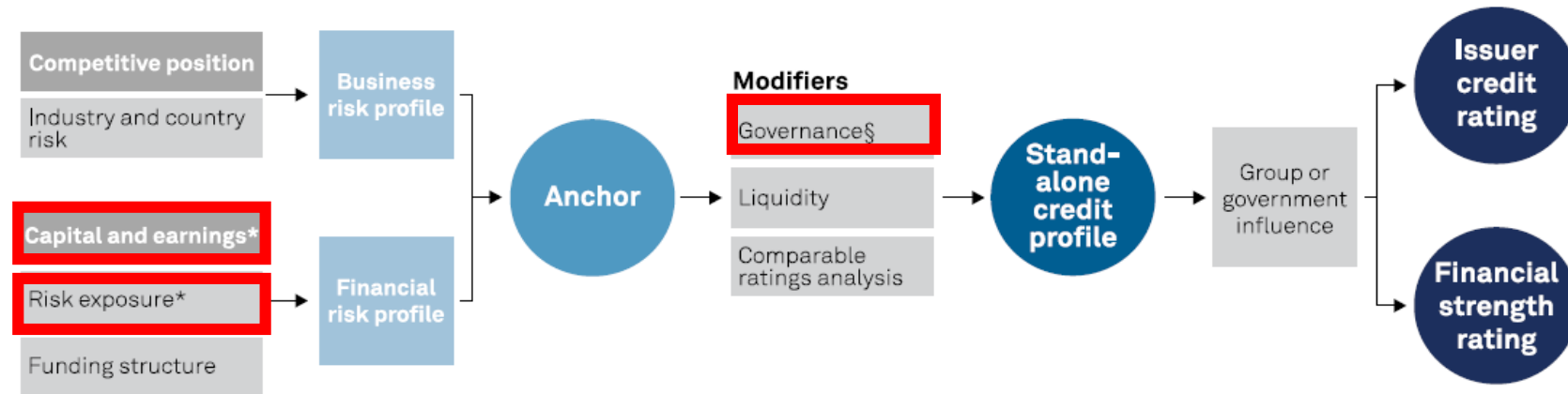
manuel.adam@spglobal.com

Insurance | 2-Sided Approach

Where is cyber captured in our analytics?

- Direct exposure considered within our wider assessment of **governance**. This assessment applies to all insurers regardless of whether they offer cyber insurance protection.
- **Governance** includes a focus on risk culture and also how internal procedures, policies and practices can create or mitigate risk, including operational risks.
- Cyber risks as part of the **business model** of some insurers in providing **cyber protection** - this is captured in our **capital modelling** and also in our assessment of **potential earnings and balance sheet volatility** (capital & risk exposure assessment).

Insurance Criteria Framework



*Factors most likely to include consideration of cyber risks as an underwriting and technical insurance risk. §Governance includes the management and handling of an insurer's own operational cyber risks. Copyright © 2020 by Standard & Poor's Financial Services LLC. All rights reserved.

Insurance | Increasing Impact Of Cyber Risks In Our Insurance Ratings

Future risks on the horizon to watch:

- 1) Too rapid an **expansion into cyber exposure** without sufficient risk and pricing considerations.
- 2) Insurers **underestimate the importance of associated cyber services** for their policyholders, such as prevention measures, crisis management and legal advice when underwriting cyber insurance. Such cyber services **strongly correlate with lower cyber claim** payments.
- 3) Reputational damage or **loss of confidence following potential outage of systems** from cyber events such that policyholders can't transact in an increasingly digital insurance world or insurers **fail to protect the sensitive data** of their stakeholders.

Type of an event for a ratings or outlook impact on an insurance company:

- 1) We detect a **material increase in risk exposure** (accumulation risk, higher policy values) or an increase in capital requirements by writing cyber insurance on a larger scale.
- 2) A **large scale global cyber event** occurs for those insurers which provide cyber insurance which may combine with other events or expand to require payouts for perils potentially in scope of coverage such as business interruption, **leading to a material capital event**.
- 3) Our cyber risk analysis highlights wider **governance deficiencies** prior to a cyber event or potentially **failure to extract risk management learnings from previous attacks**.

Cyber Risk In A New Era

Cyber Risk Analytics

Financial Institutions

Irina Velieva

Director

S&P Global Ratings

irina.velieva@spglobal.com

Financial Institutions | Cyber Risks and Bank Ratings

Where is cyber captured in our analytics?

We believe **that banks are clear targets for cyber-attacks**, since they usually have a lot of sensitive customer data. A successful cyber attack on a bank could cause reputational, legal and monetary damages.

General focus area:

- We look at the bank's ability to manage and prevent cyber risks as a part of our broader risk management and governance assessment. We consider the bank's inability to manage and control cyber risks could weaken its overall risk profile.

If a successful attack occurred:

- Successful cyber-attacks may impair customer loyalty and expose the bank to franchise volatility and unstable earnings.
- Reputational damages from cyber events may result in the loss of customer confidence and cause the outflow of clients' funds.
- Potential losses from cyber events, as well as possible regulatory fines, could hurt bank's profitability and capital.

We can also capture cyber-risks as a part of our system-wide banking sector analysis in a given country, in cases when the banking industry as a whole suffers from a series of repeated, serious breaches of security.

Financial Institutions | Cyber Risks and Bank Ratings

Case study

In February 2019, Bank of Valetta suffered from an attack targeting its international payment system. We viewed that as another challenge for the bank to defend its reputation and to prove its IT and compliance monitoring tools are robust and efficient.

At that stage, the bank's ratings were already on negative outlook, reflecting the risk that its ongoing litigation cases could tarnish its reputation and ultimately affect its business and financial profiles. The cyber attack was another setback the bank had to overcome. In July 2019, we have downgraded the bank from BBB/Neg/A-2 to BBB-/Stable/A-3 on increased doubts regarding the robustness of the bank's operational risk management.

Summary

Although the bank's vulnerability to cyber risks is rarely the single factor for a rating movement, exposure to cyber risks, losses from attacks and management's track record can be one of the decisive factors for any rating outcome.

Cyber Risk In A New Era

Cyber Risk Analytics

Structured Finance

Matthew Mitchell

Director

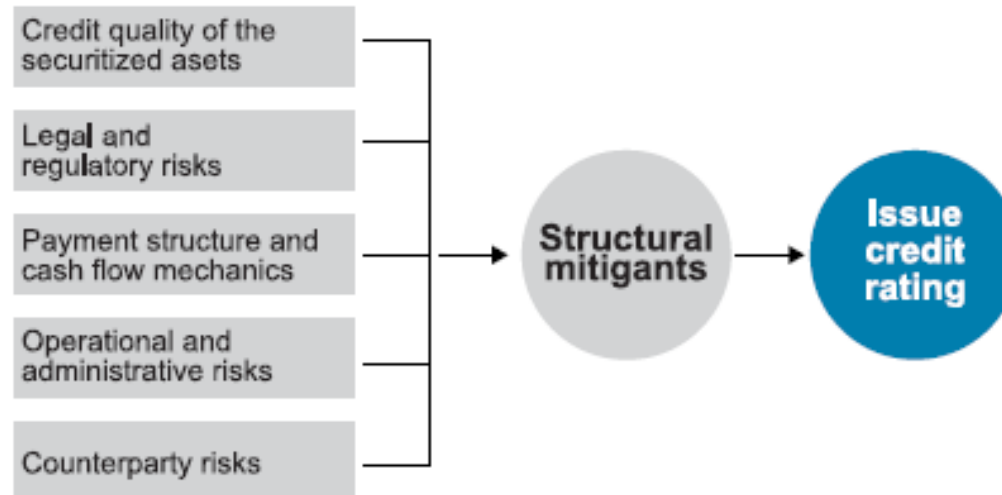
S&P Global Ratings

matthew.mitchell@spglobal.com

Structured Finance | Cyber Typically An Indirect Risk

Where is cyber captured in our analytics?

- Cyber risks are typically indirect exposures for structured finance transactions. Given that issuers are established as special purpose entities (SPE), cyber threats are more likely to impact one of the related transaction parties, such as the originator or servicer.
- We consider cyber risks as a **governance** credit factor under our ESG framework.
- We believe consumer receivables would be more exposed to potential legal or regulatory action following a data breach than commercial receivables.



Cyber Risk In A New Era

Cyber Risk Analytics

Methodologies

Cristina Polizu

Managing Director

S&P Global Ratings

cristina.polizu@spglobal.com

Key Takeaways And Companies Included

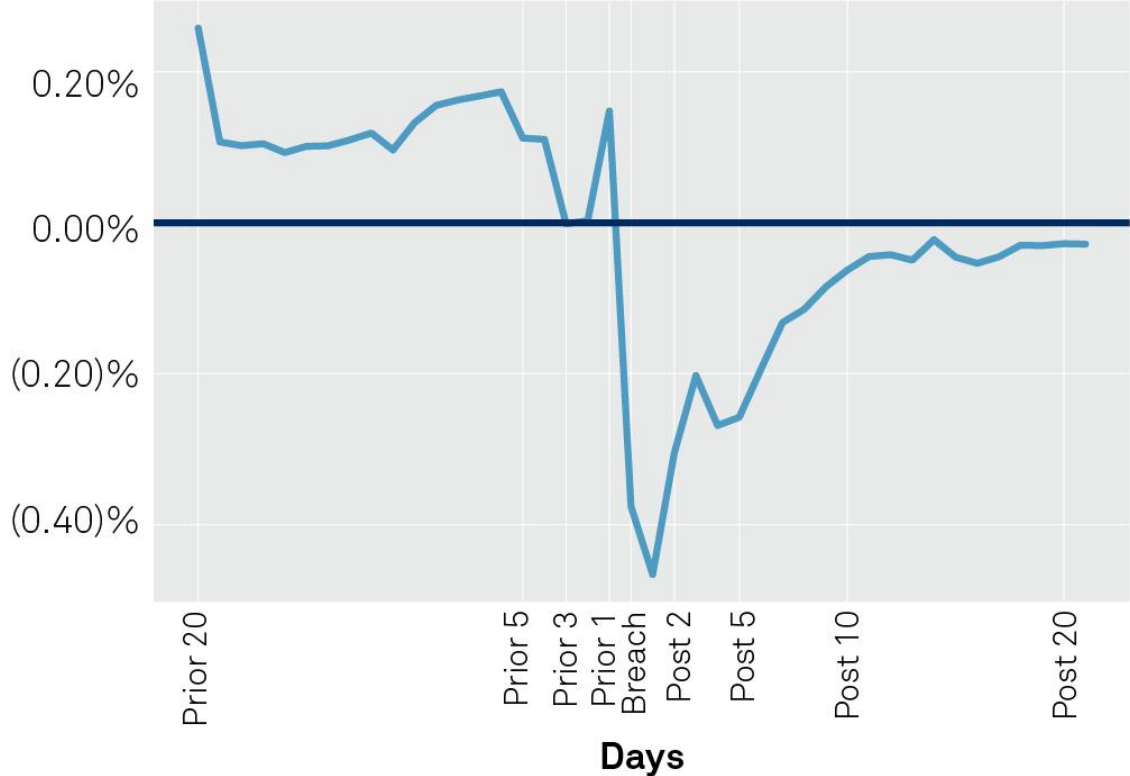
- We analysed cyberattacks (data breaches) since 2007 to 2019 for 32 rated companies for a total of 41 events—as reported on Google News.
 - We found that the data breaches didn't have a lasting effect on revenue and EBITDA.
 - However, they may weaken equity prices and widen credit default swap spreads in the short term.
 - The study does not cover non data breach cyber events the analysis of which may lead to a different conclusion.
 - Cyber events may impact credit worthiness if material and expose previously undetected governance weaknesses.
-
- Technology: Apple, Adobe, Microsoft, Sony, T-Mobile, Vodafone, and Verizon.
 - Financial Institutions: Citigroup, Capital One, First American Financial, JPMorgan Chase, and Wells Fargo.
 - Corporates: Anthem, Boeing, Community Health Systems, Delta, Equifax, Quest Diagnostics, Disney, eBay, Global Payments, Home Depot, Health Net, Marriott, Rite Aid, Staples, Target, TJ Maxx, Under Armour, Walmart, and British Airways.

Findings

- **Equity prices:** Most data breach events cause a drop in equity prices after the event has been reported in the news, which rebound and normalize in subsequent weeks.
- **CDS spreads:** Some data breach events may cause a rise in spreads after the event is reported, which normalize in subsequent weeks.
- **Financial ratios:** We did not see clear evidence of quarterly deterioration when analyzing the impact on revenue and EBITDA. Due to the nature of quarterly reporting, that may give time for companies to mitigate any effects on financials.
- We found only half of the events in the studied sample in filings to the U.S. Securities and Exchange Commission.

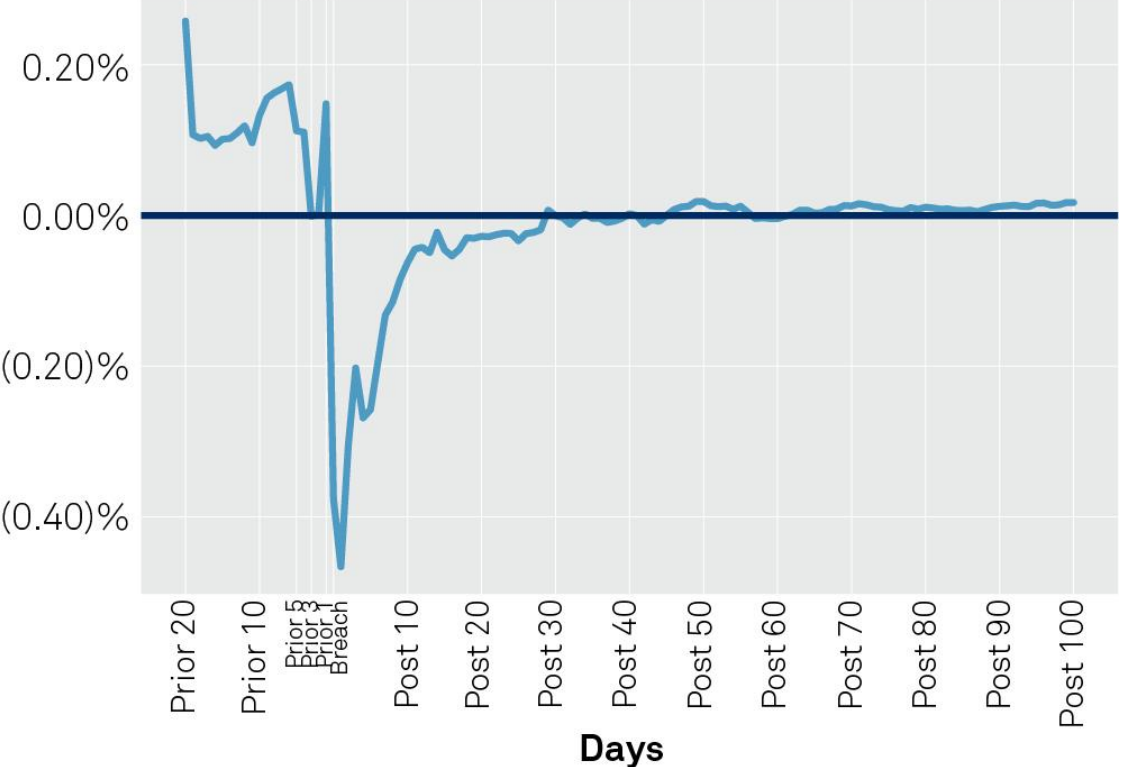
The Average Equity Price Return Was Close To -0.5% The Day After Data Breach Event

The average equity price return 20 days before and after the day of breach event



Source: Compustat, S&P Global Market Intelligence.

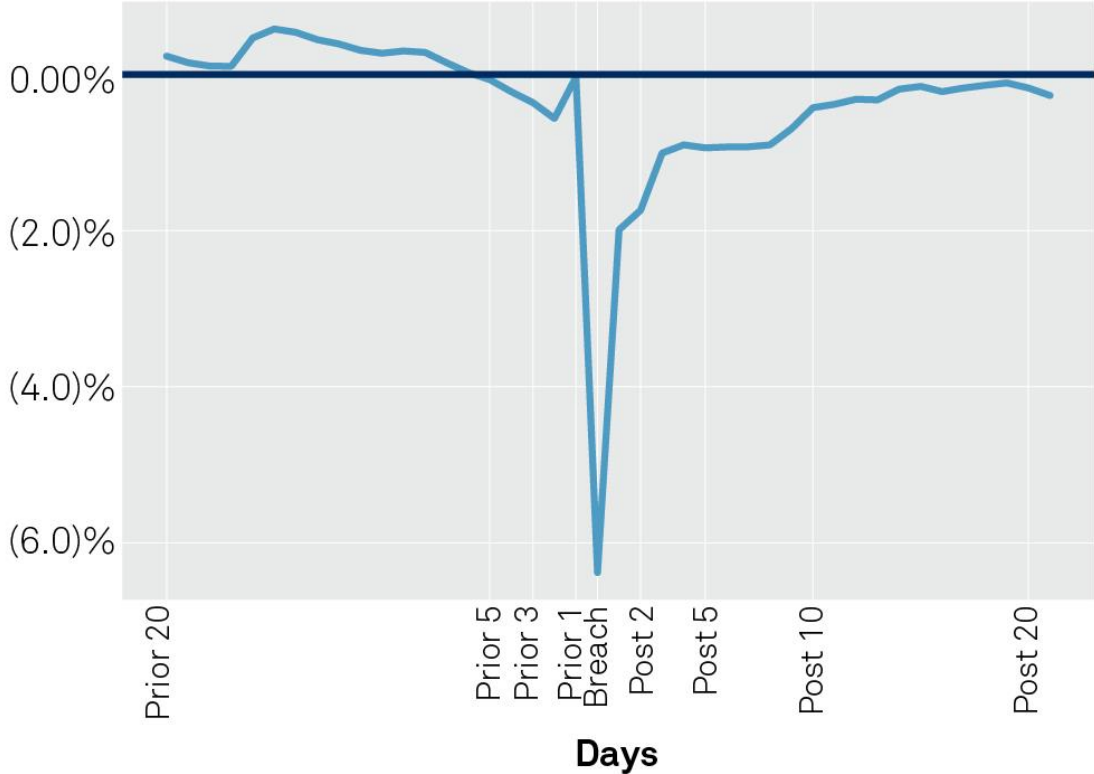
The average equity price return 20 days before and 100 days after the day of breach event



Source: Compustat, S&P Global Market Intelligence.

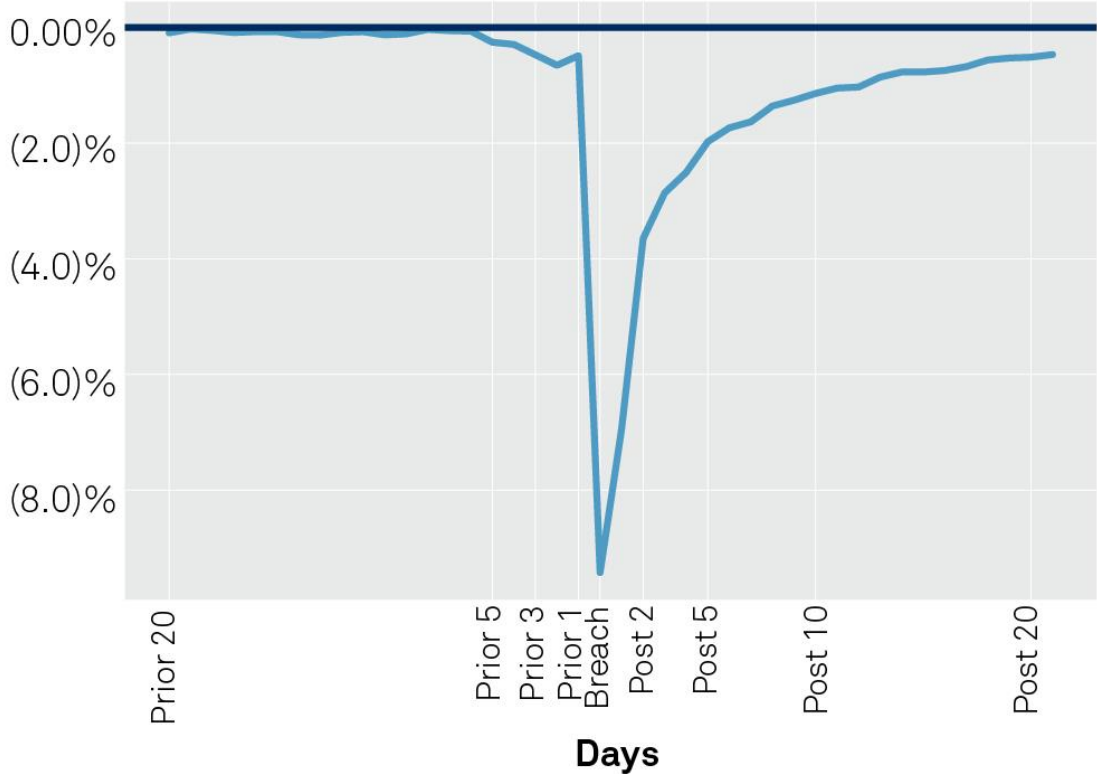
Marriott And Global Payments Showed The Largest Drops In Equity Price Returns, During the Breach Events

Marriott – average abnormal stock return



Source: Compustat, S&P Global Market Intelligence.

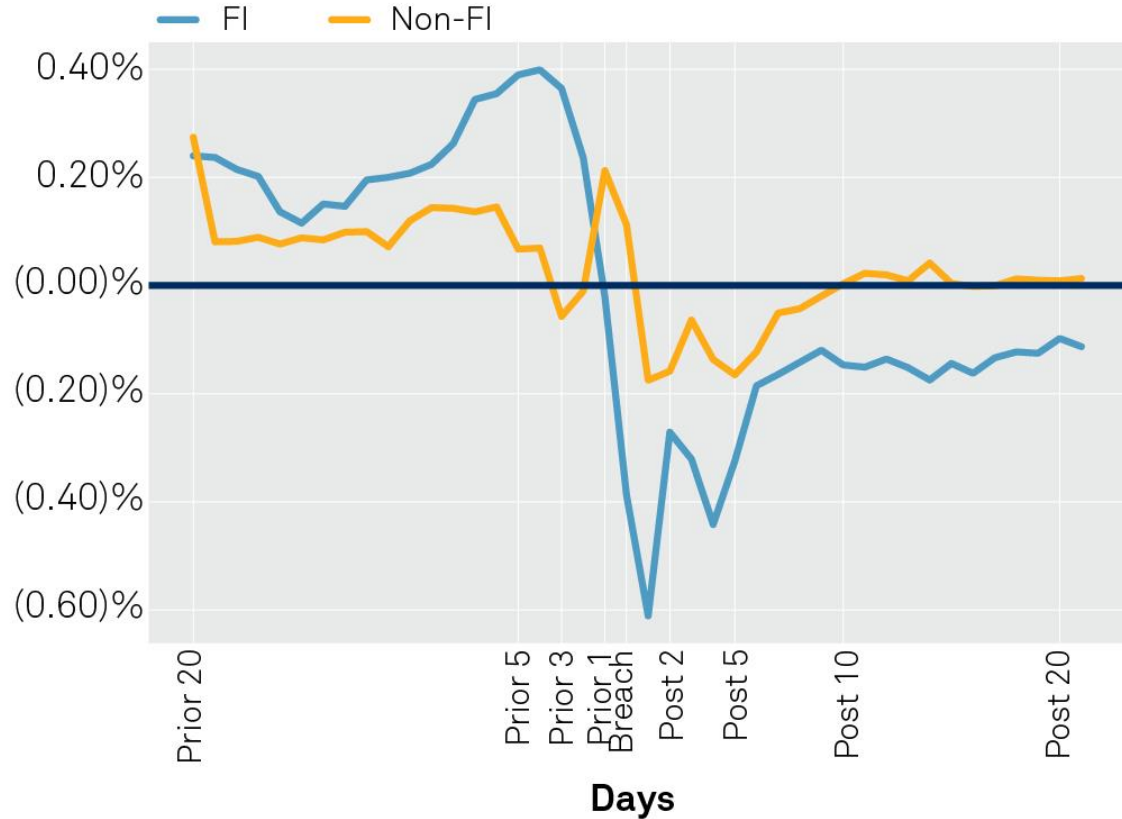
Global Payments – average abnormal stock return



Source: Compustat, S&P Global Market Intelligence.

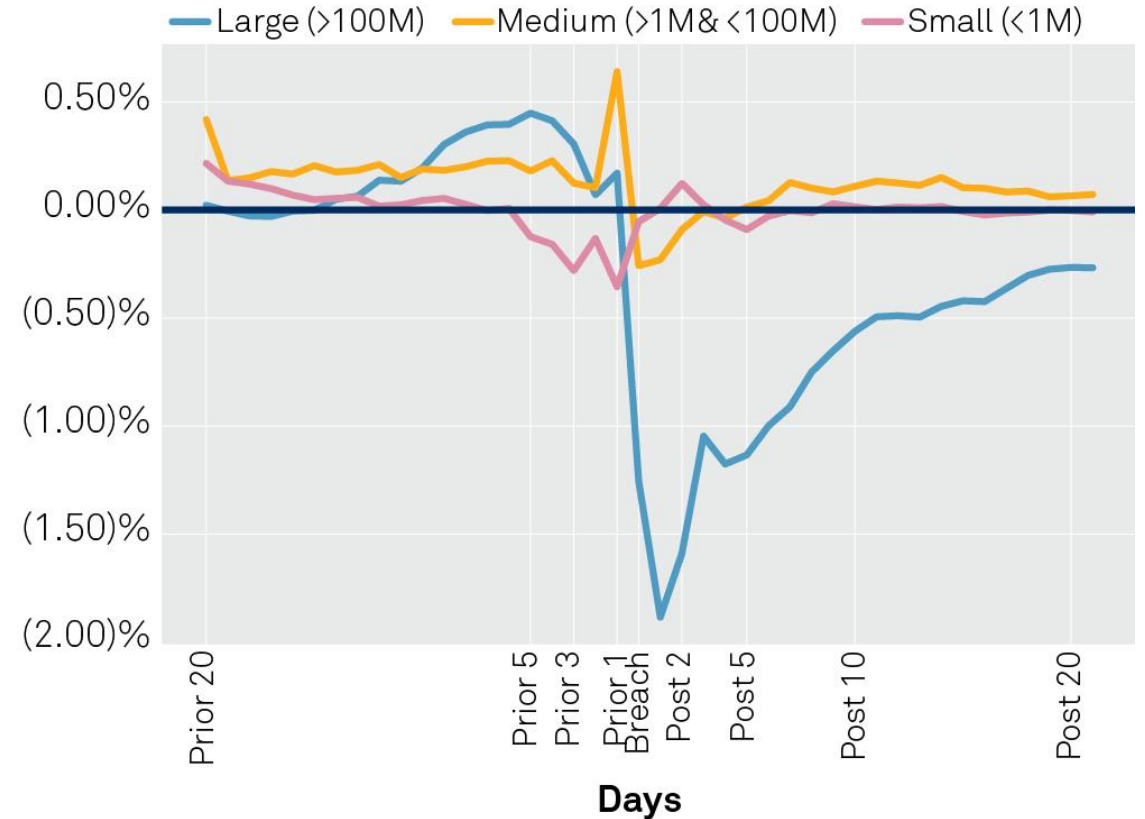
Large Breaches And The Financial Institutions Sector Experienced Sharper Declines

Equity price returns declined more sharply for financial institutions (FI)



Source: Compustat, S&P Global Market Intelligence.

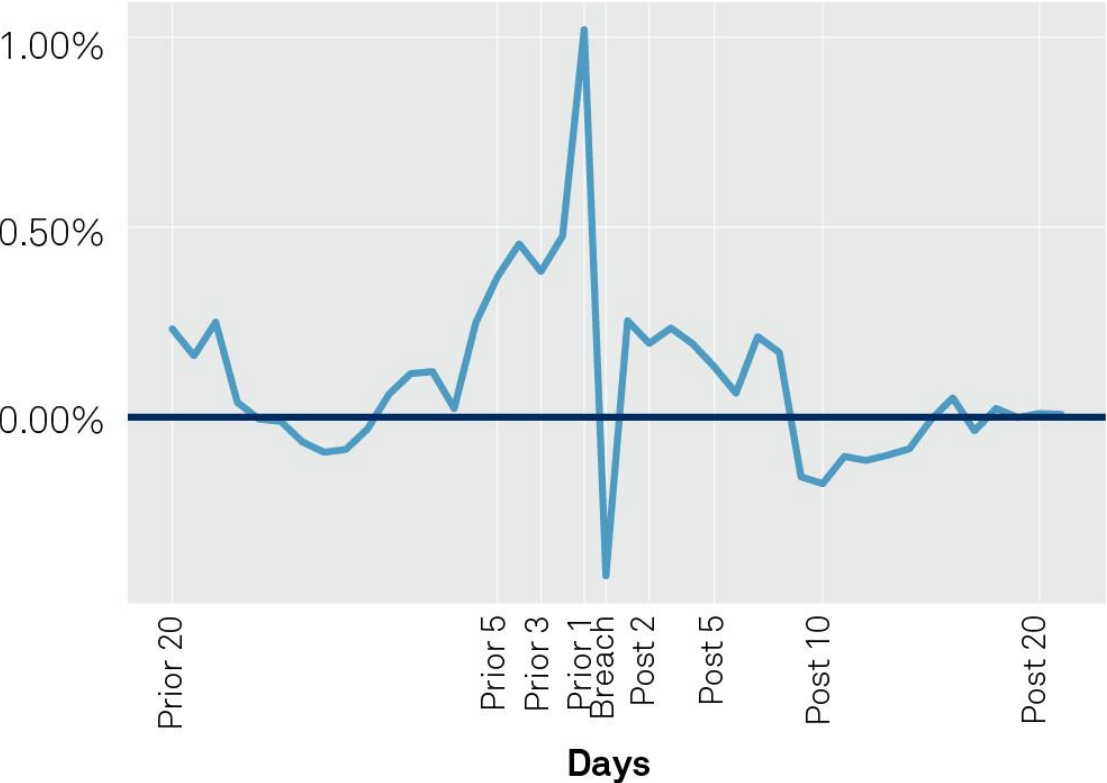
Equity price returns declined more sharply for companies with large breaches



Source: Compustat, S&P Global Market Intelligence.

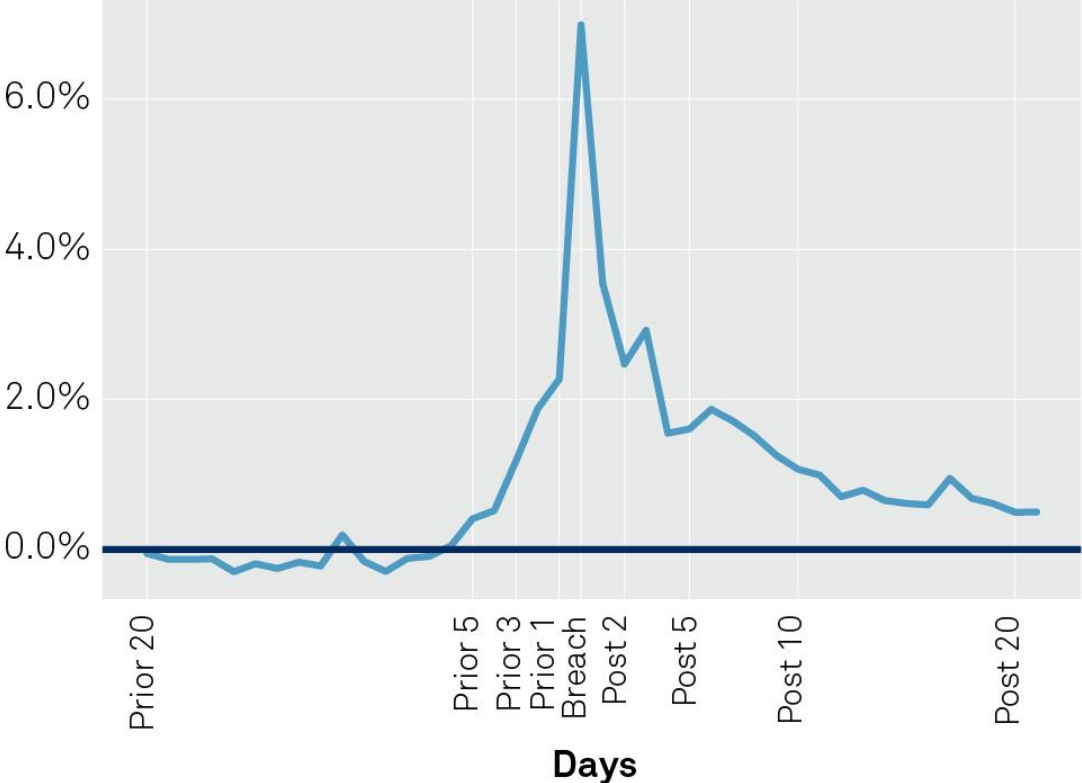
CDS Spreads Widen 0.2% On Average One Day After Data Breach

CDS spread percent changes 20 days prior and after day of data breach



CDS data was available for 20 events (17 companies). Source: S&P Global Ratings, Intercontinental Exchange Credit Market Analysis (ICE CMA)

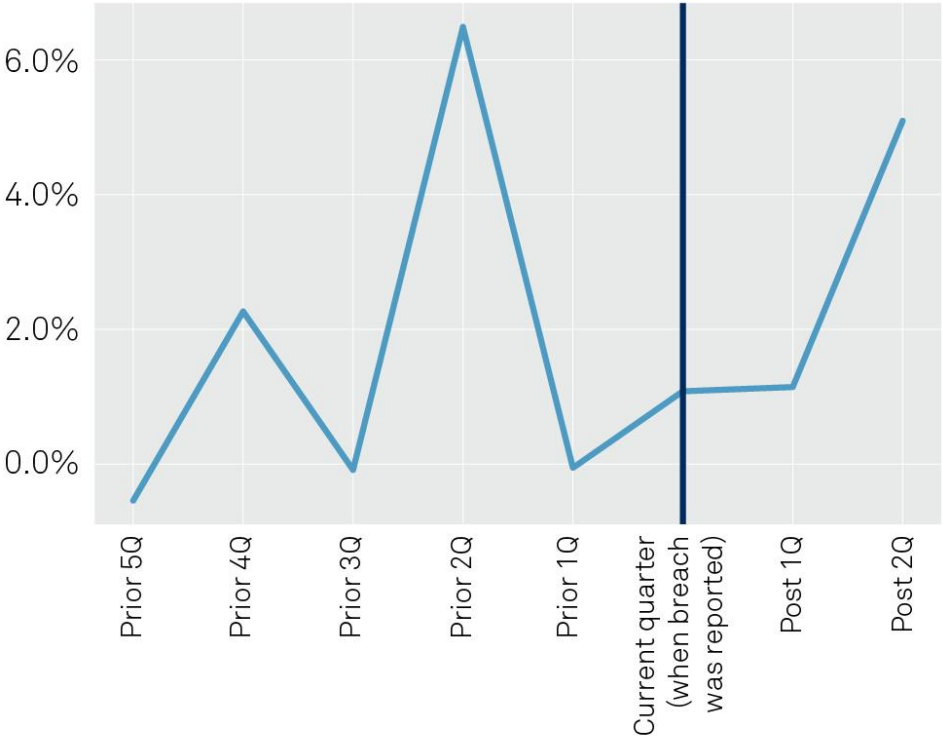
CDS spread percent changes 20 days prior and after day of data breach (Marriott)



Source: S&P Global Ratings, Intercontinental Exchange Credit Market Analysis (ICE CMA)

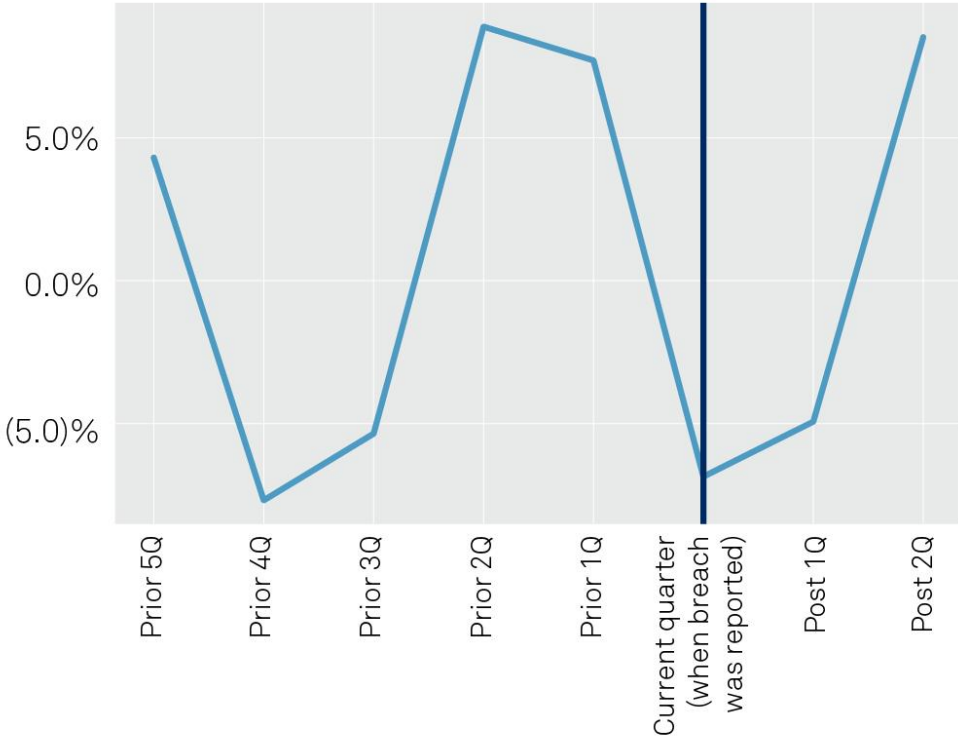
We See No Clear Evidence Of Declines In Quarterly Revenue Attributed To Data Breaches

Average quarterly revenue changes in the five quarters prior and two quarters after the data breach



The average above is based on 35 events with quarterly data. Source: S&P Global Ratings

Some companies saw revenue decline in the quarter of the data breach and subsequent quarter, but those could be seasonal effects

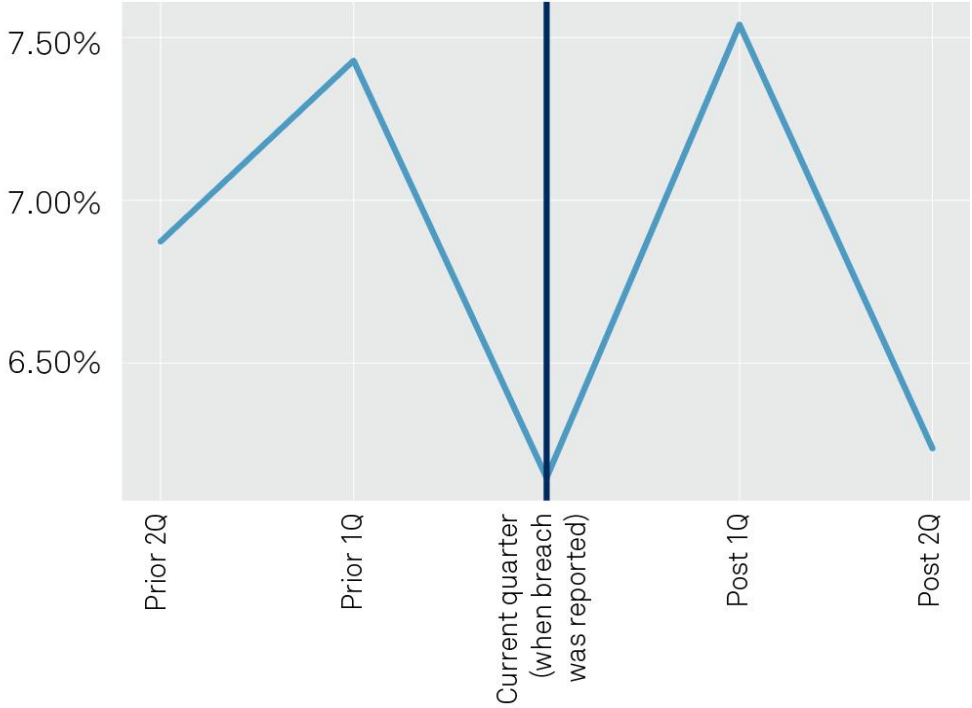


Source: S&P Global Ratings.

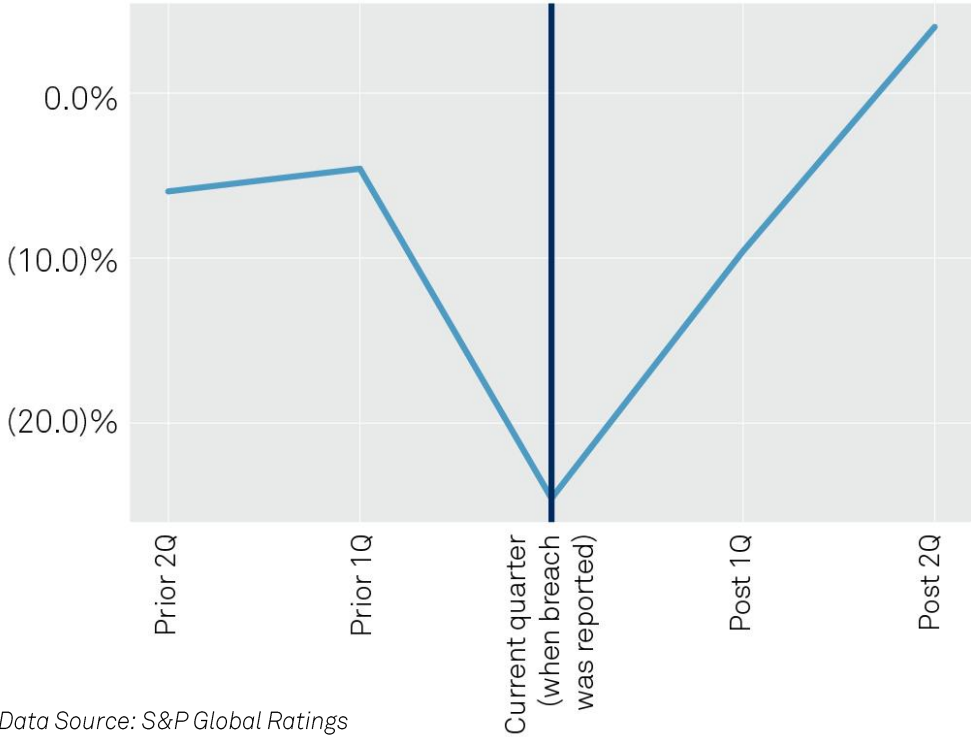
We See No Clear Relationship Between Year-On-Year Changes In Quarterly Revenue And Data Breach Events

- On average, returns remained positive, but some companies saw declines in revenue.
- We believe companies that handle cyberattacks well can manage and maintain revenue in the aftermath of an attack.

Average changes in quarterly revenue are non-negative year on year



Some companies saw drops in revenue in the quarter the breach was reported and in the subsequent quarter

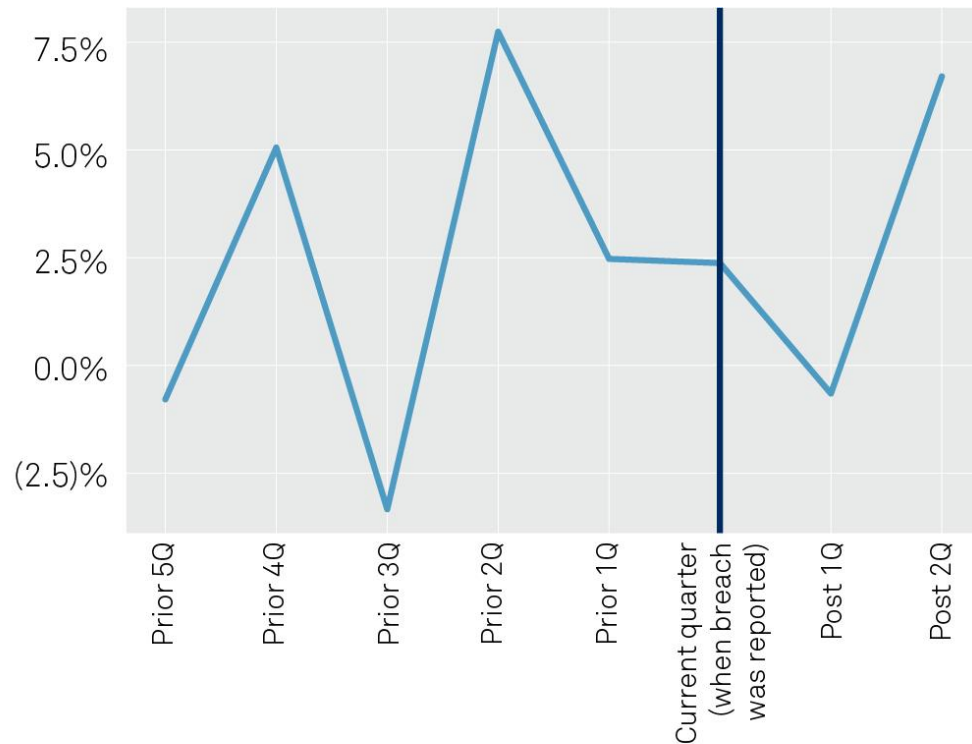


The average above is based on 36 events. Data Source: S&P Global Ratings

Data Source: S&P Global Ratings

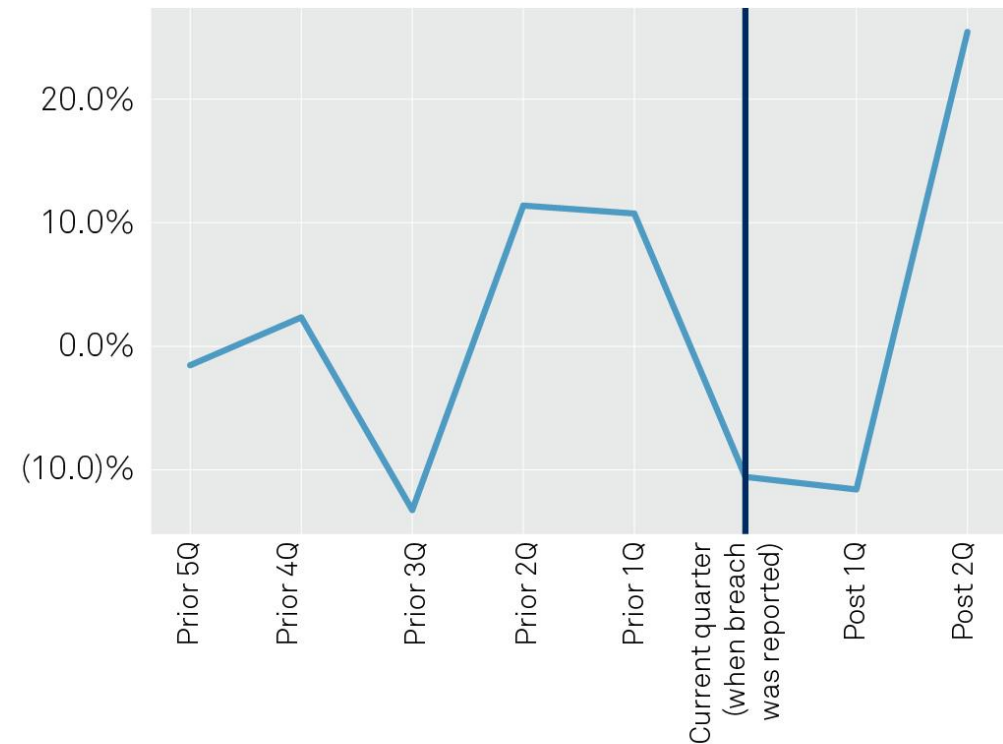
We See No Clear Negative Relationship Between Quarterly Changes In EBITDA And Data Breaches

Average changes in quarterly EBITDA in the five quarters before and the two quarters after the data breach



The average above is based on 29 events with quarterly data. Selected outliers are excluded.
Data Source: S&P Global Ratings

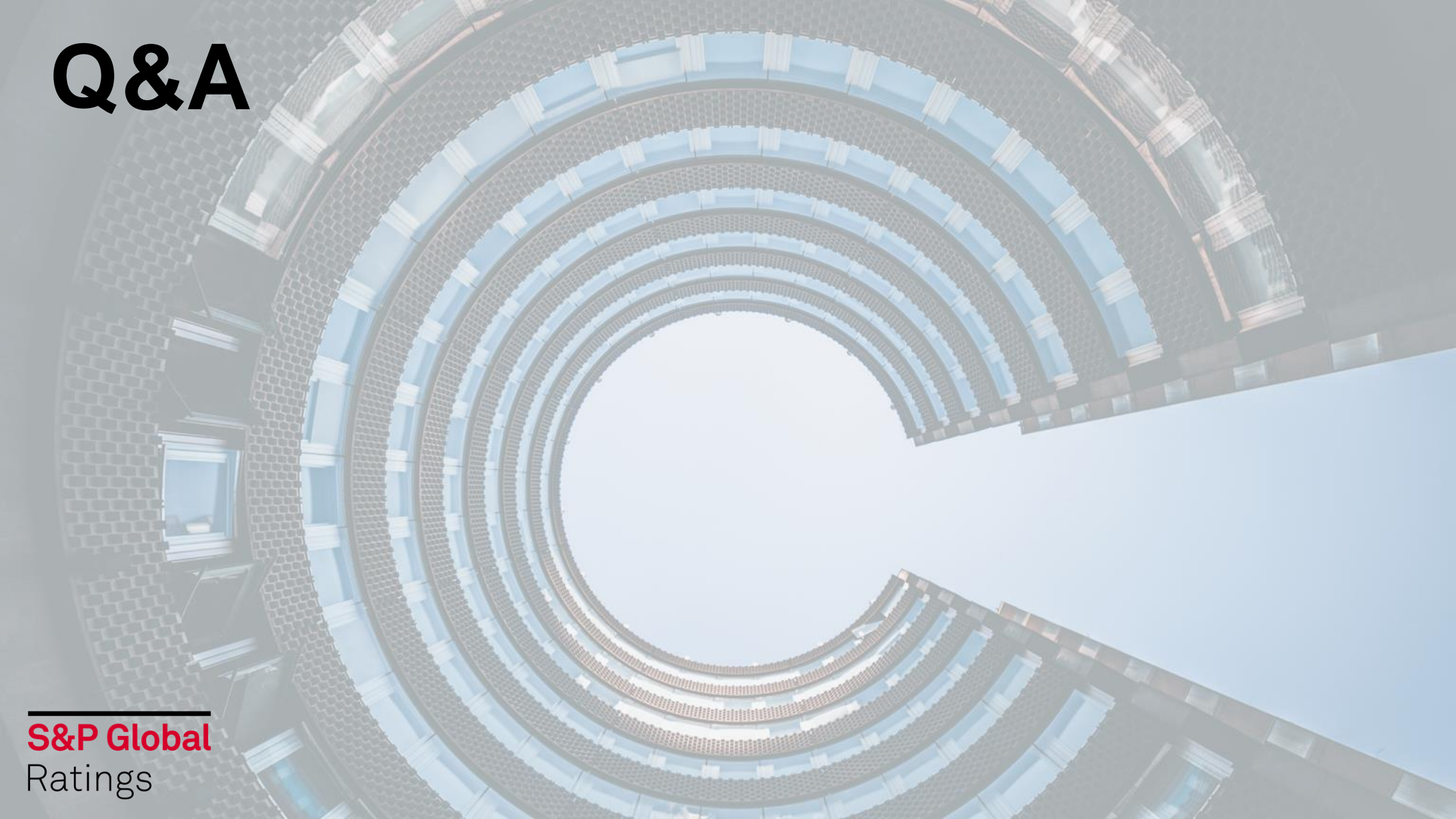
Some companies saw drops in EBITDA in the quarter of the breach and one quarter after, but those could be seasonal effects



Data Source: S&P Global Ratings

Q&A

S&P Global
Ratings



Copyright © 2020 by Standard & Poor's Financial Services LLC. All rights reserved.

No content (including ratings, credit-related analyses and data, valuations, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of Standard & Poor's Financial Services LLC or its affiliates (collectively, S&P). The Content shall not be used for any unlawful or unauthorized purposes. S&P and any third-party providers, as well as their directors, officers, shareholders, employees or agents (collectively S&P Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Parties are not responsible for any errors or omissions (negligent or otherwise), regardless of the cause, for the results obtained from the use of the Content, or for the security or maintenance of any data input by the user. The Content is provided on an "as is" basis. S&P PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

Credit-related and other analyses, including ratings, and statements in the Content are statements of opinion as of the date they are expressed and not statements of fact. S&P's opinions, analyses and rating acknowledgment decisions (described below) are not recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P does not act as a fiduciary or an investment advisor except where registered as such. While S&P has obtained information from sources it believes to be reliable, S&P does not perform an audit and undertakes no duty of due diligence or independent verification of any information it receives.

To the extent that regulatory authorities allow a rating agency to acknowledge in one jurisdiction a rating issued in another jurisdiction for certain regulatory purposes, S&P reserves the right to assign, withdraw or suspend such acknowledgement at any time and in its sole discretion. S&P Parties disclaim any duty whatsoever arising out of the assignment, withdrawal or suspension of an acknowledgment as well as any liability for any damage alleged to have been suffered on account thereof.

S&P keeps certain activities of its business units separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain business units of S&P may have information that is not available to other S&P business units. S&P has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P reserves the right to disseminate its opinions and analyses. S&P's public ratings and analyses are made available on its Web sites, www.standardandpoors.com (free of charge), and www.ratingsdirect.com and www.globalcreditportal.com (subscription), and may be distributed through other means, including via S&P publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.

Australia

Standard & Poor's (Australia) Pty. Ltd. holds Australian financial services license number 337565 under the Corporations Act 2001. Standard & Poor's credit ratings and related research are not intended for and must not be distributed to any person in Australia other than a wholesale client (as defined in Chapter 7 of the Corporations Act).

STANDARD & POOR'S, S&P and RATINGSDIRECT are registered trademarks of Standard & Poor's Financial Services LLC.