SUSTAINALYTICS
a Morningstar company

MORNINGSTAR®

Data Privacy and Security

Beyond breaches: why this dynamic ESG issue should be on your radar.

Morningstar Equity Research
June 27, 2022

Contents

Emma Williams
Equity Analyst, ESG
Morningstar
+1 312-244-7640
emma.williams@morningstar.com

Melissa Hudson
Associate Director, Privacy & Cybersecurity
Sustainalytics
+1 416 861 0403
Melissa.hudson@morningstar.com

Tiffany Flaherty
Manager, ESG Research, Risk Rating Oversight
Sustainalytics
+31 20 205 0000
tiffany.flaherty@morningstar.com

Livia Toni
Senior Analyst, ESG Research
Sustainalytics
+49 69 50607618
livia.toni@morningstar.com

Executive Summary

In an increasingly interconnected and digitized world fueled by mega trends such as the "Internet of Things," cloud computing, and accelerated digitization during the COVID-19 pandemic, companies across a broad range of subindustries are grappling with heightened exposure to data privacy and security, or DP&S, risk. Digitization has become a double-edged sword for business—it is a key driver of operational efficiencies and growth opportunities, while simultaneously creating more points of entry for bad actors to steal customer data or cause operational disruption through malicious activities.

While the ability to collect and aggregate customer data aids personalized services, customer engagement, marketing, and research and development activities, companies are increasingly exposed to a myriad of risks and greater responsibility to safeguard digital assets. These risks extend beyond data breaches and cybersecurity threats and the associated ramifications, including reputational damage or lost business. They also include regulatory penalties and societal scrutiny of controversial or unlawful use, or disclosure of customers' personal information through practices such as data monetization.

So how can investors understand the extent of a company's exposure to DP&S risk? We see three key drivers of risk exposure at the subindustry level: the processing of customers' personal information, the surface area of attack, and whether the subindustry consists of critical infrastructure. Taken together, these risk drivers demonstrate the varied avenues by which bad actors can exploit companies, threaten data privacy protection, cause operational disruption, and inflict reputational damage. In addition to the subindustry-level risk drivers, we recommend investors consider two key drivers at a company level—involvement in data monetization and the supply chain of service providers.

While a systematic increase in DP&S risk can create upside opportunities for certain companies such as those providing cybersecurity software, we focus primarily on downside risk at a subindustry level. However, we highlight the importance of company-level risk mitigation measures and competitive positioning when assessing valuation impact.

Key Takeaways

- Data breaches are high-profile impacts of DP&S risk, but impacts extend far beyond this, including regulatory and societal scrutiny of controversial or unlawful use, or disclosure of data.
- Our analysis indicates that the telecommunication services, insurance brokers, and internet software and services subindustries are most exposed to DP&S risk.

- During the COVID-19 pandemic, many industries were forced to undergo accelerated digitization, which in turn increased their attack surface and DP&S risk profile.
- At the extreme, regulatory scrutiny of data monetization practices could threaten entire business models such as that of data brokers and primary, or at least high-margin, revenue streams for big-tech providers such as Meta Platforms, Alphabet, and Amazon.
- Corporates, investors, and insurers are struggling to measure and counter DP&S risk, but we offer a pragmatic model to holistically assess exposure despite limited data disclosure.

Companies Mentioned

Name/Ticker	ESG Risk Rating	Economic Moat	Currency	Fair Value Estimate	Current Price	Uncertainty Rating	Morningstar Rating	Market Cap (USD Bil)
Adobe Systems/ADBE	Low	Wide	USD	500	377	Medium	★★★★	173
Alphabet/GOOGL	Medium	Wide	USD	3,600	2,245	High	★★★★	1,472
Amazon.com/AMZN	High	Wide	USD	192	112	High	★★★★★	1,109
Anheuser-Busch InBev/ABI	Medium	Wide	EUR	80	50	Medium	★★★★★	91
Apple/AAPL	Low	Narrow	USD	130	138	High	★★★	2,191
Dropbox/DBX	Low	None	USD	26	22	Very High	★★★★	8
Imperial Brands/IMB	Medium	Wide	GBX	2,900	1,817	Medium	★★★★★	21
Meta Platforms/META	High	Wide	USD	384	159	High	★★★★★	422
Millicom International/TIGO	Low	Narrow	USD	34	15	High	★★★★★	2
PayPal Holdings/PYPL	Low	Narrow	USD	139	74	High	★★★★★	85
Polaris (US)/PII	Low	Wide	USD	175	104	High	★★★★★	6
Prudential UK/PRU	Low	None	GBX	1,480	935	Medium	★★★★★	31
Target (US)/TGT	Low	None	USD	171	147	Medium	★★★★	65
Tencent Holdings/00700	Medium	Wide	HKD	741	375	High	★★★★★	460

What Is DP&S Risk, and Why Does It Matter?

Data privacy- and cybersecurity-related issues have become major drivers of business risk in the past several years. As companies digitize and business models shift toward complex data-driven products and services, stakeholders are reckoning with a significant realignment in global risk. Recent events highlight the rising stakes of DP&S risk. These include a rapid increase in cyber incidents during COVID-19, in part fueled by a shift to remote work; the SolarWinds supply chain attack, which demonstrated the scale of interdependence in the digital ecosystem; the Colonial Pipeline attack, highlighting the vulnerability of critical infrastructure; and the Russian invasion of Ukraine increasing awareness of the real possibility of cyber sabotage.

Personal information has become an essential commodity, and the cost of failing to protect it continues to increase as customer awareness grows in time with more stringent privacy laws and more assertive enforcement. With the introduction of the General Data Protection Regulation, or GDPR, and the California Consumer Privacy Act, or CCPA, we are seeing a process of convergence in comprehensive privacy legislation. EY's 2021 Global Information Security Survey[1] found that 77% of organizations have seen an increase in disruptive attacks in the last 12 months, up from 59% in the previous survey. More than half of respondents expressed that cybersecurity is under more scrutiny than at any time before. Morningstar Sustainalytics' own data bears this out—the number of privacy and cybersecurity incidents have seen an upward trend since 2016, with a significant acceleration since 2018.

The financial impact of DP&S incidents can be significant, so much so that the cybersecurity insurance industry is struggling to keep up—the cost of coverage in the U.S. more than doubled in the fourth quarter of 2021 alone.[2] In addition to rising compliance costs, there have been several high-profile penalties in recent years, including Amazon's EUR 746 million fine for breaching the GDPR in 2021, as well as Facebook's USD 5 billion settlement with the Federal Trade Commission, or FTC, in 2019. The latter is one of the largest penalties ever assessed by the U.S. government for *any* violation and includes highly prescriptive changes to related corporate governance, enhanced privacy measures, quarterly attestations to the FTC, and the appointment of an independent assessor, with such measures to remain in place for 20 years.[3] Clearly, the cost of a DP&S incident exceeds—often far exceeds—the cost of a financial penalty. These costs include expenditures to investigate and respond to an incident, costs associated with system downtime including revenue and customer losses, customer remediation costs, and regulatory fines. It is equally important to recognize the financial, regulatory, and reputational risks that arise not just from cyberthreats and data breaches but also from concerns around perceived misuse and/or lack of transparency. We see a corresponding pattern when we look at reported financial damages reported by cyberattack specialist organizations. For example, McAfee estimated the average cost of cybercrime at $475 billion in 2014, $523 billion by 2018, and $945 billion by 2020.[4]

1 https://www.ey.com/en_nl/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

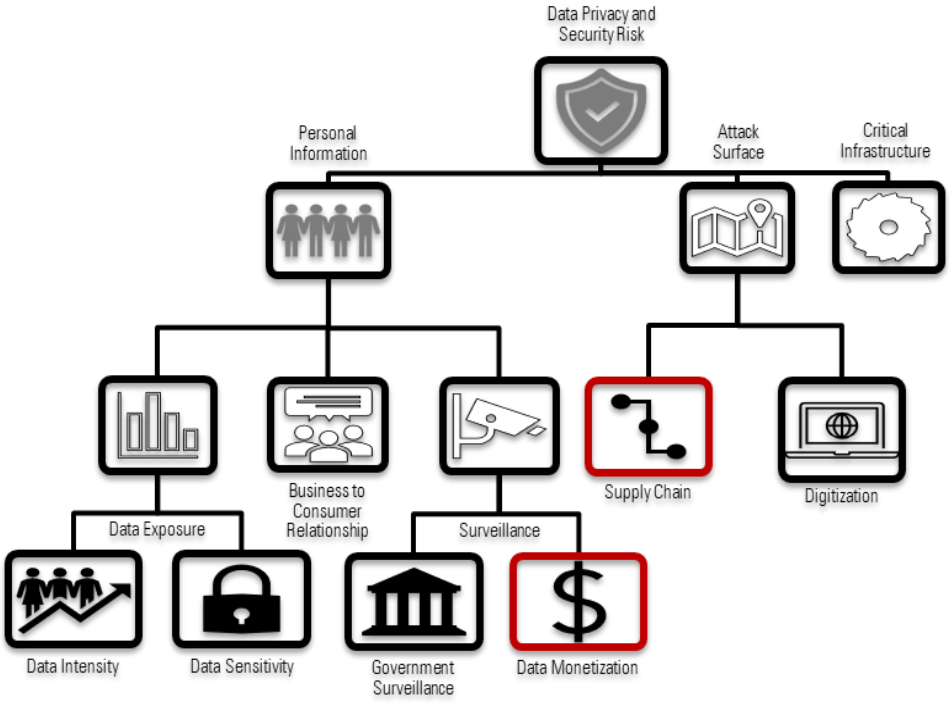
2 https://www.ft.com/content/60ddc050-a846-461a-aa10-5aaabf6b35a5

3 https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

4 https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

The Three Key Components of DP&S Risk: Privacy, Attack Surface, and Critical Infrastructure

Exhibit 1A: A Company's Exposure to DP&S Risk Can Be Assessed Using Our Risk Driver Framework



Source: Morningstar, Morningstar Sustainalytics.
Note: The supply chain and data monetization risk drivers are more appropriately assessed at a company level, the remainder can be assessed at a subindustry level.

To establish and validate our DP&S risk exposure framework, we established a proprietary dataset[5] that scores subindustries on our underlying risk drivers. This dataset is informed by Sustainalytics and Morningstar data, industry expertise, reputable industry studies, and standard-setting legislation.[6]

When establishing the scope of our data privacy and security risk framework, we focus on *privacy* first, namely the collection and safeguarding of customers' personally identifiable information, or PII, collected during a company's normal course of business. While we acknowledge that protecting the confidentiality of all information that a company processes (including business secrets and intellectual property) is critical, PII is unique with respect to data protection. Research from the IBM/Ponemon Institute survey indicates personally identifiable information is by far the most common type of data compromised in breaches and the most valuable. As a result, our framework for assessing data privacy and security risk puts PII front and center, including when assessing data sensitivity, data intensity, risk related to business-to-consumer relationships, data monetization, and government surveillance.

5 See Appendix for more detail.

6 See "Investors Should Push for More DP&S Risk Data" section.

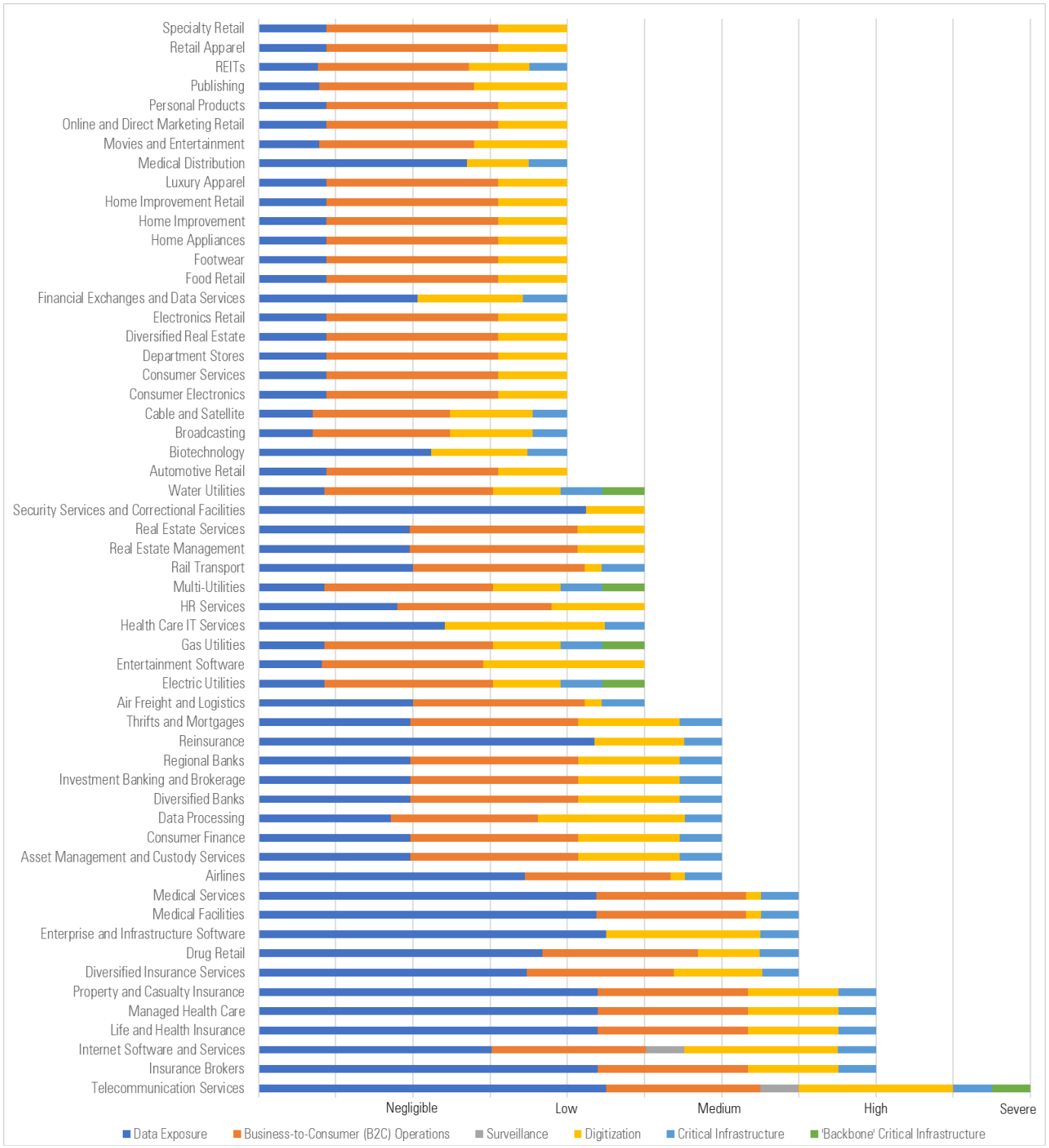
Our second dimension is assessing the "attack surface." Digitization acts as a double-edged sword—it is a key business driver that is also associated, all things equal, with more points of entry for bad actors to steal customer data or cause operational disruption through malicious activities. Beyond the degree to which a company is vulnerable to attack via its own technical infrastructure, this dimension of risk also includes what we call the "digital supply chain," namely technology that a company purchases or licenses from a third party, which in turn makes it vulnerable to a supply chain attack, such as the notorious SolarWinds hack in 2020 that Microsoft's CEO referred to as "the largest and most sophisticated attack the world has ever seen."[7] In addition, we consider the standard service-provider supply chain within this dimension—when companies outsource activities that involve granting third parties access to PII, they are increasing their attack surface with respect to that data.

Finally, certain subindustries have innate characteristics that increase DP&S risk, namely their identification by national governments as critical infrastructure, or CI. CI consists of sectors identified as essential to the functioning of the economy and state. Each of these sectors is subject to what is often referred to as "critical infrastructure protection" that reflects their strategic and prestige value to bad actors. While there is no international consensus on what constitutes CI—for example, the U.S. identifies 16 sectors that constitute CI, while the U.K. has 13—this generally includes what we call "backbone critical infrastructure," or industries that are seen to form a single point of failure in an economy, including communications, utilities, energy, and transportation. As a recent example, the 2021 shutdown of the Colonial Pipeline is seen as a game-changing attack on critical infrastructure.

We have used the above-mentioned risk drivers to holistically assess subindustry-level exposure to DP&S risk. As shown in Exhibit 1, we consider telecommunications as the riskiest industry, closely followed by insurance, software and services, and healthcare.

7 https://www.businessinsider.com/microsoft-solarwinds-attack-hack-russia-nobelium-targets-government-agencies-ngo-2021-5

Exhibit 1 Investors Should Consider a Holistic Set of Risk Drivers When Assessing DP&S Exposure



Source: Morningstar, Morningstar Sustainalytics.
Note: Data excludes subindustries with negligible or low exposure to DP&S risk.

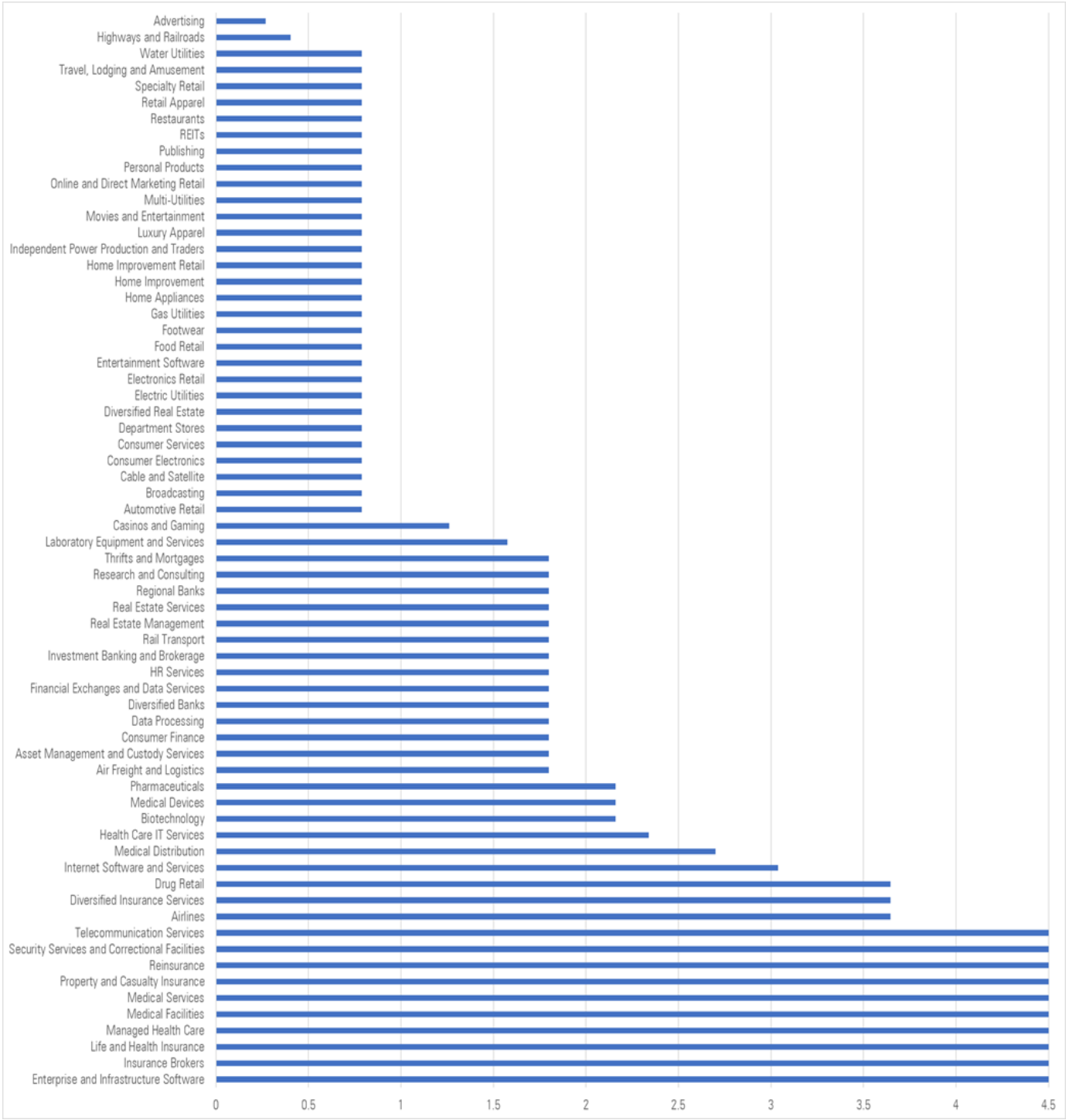
Data Exposure: The Core Driver of DP&S Risk

The cornerstone drivers for data privacy and security risk are the volume and sensitivity of data processed. In virtually all consumer-facing subindustries, companies collect masses of data points through either voluntary disclosure or more insidious tracking devices. Beyond collecting and processing data for normal operations, this data can be leveraged to inform targeted advertising, product development, or be sold on to third parties such as data brokers. Companies with high data exposure are both more attractive to hackers and more likely to face regulatory risk or public scrutiny related to inappropriate or unlawful data use or disclosure. These companies are also more susceptible to malicious attacks aimed at stealing data or taking servers offline.

To assess this element of risk exposure, we believe that the data intensity—meaning the number of data points collected on each data subject—needs to be assessed in conjunction with the data sensitivity of data processed. In practice, we expect the risk and potential cost of a data breach is magnified if a company deals with both large volumes of data and highly sensitive data. By contrast, we expect companies processing large volumes of data that is nonsensitive or even publicly available will be less attractive to a hacker. To measure this, we have developed a data exposure score, which is the product of data intensity and data sensitivity of customers' personal information processed during normal operations.

As seen in Exhibit 2, our analysis indicates that the enterprise and infrastructure software, insurance brokers, life and health insurance, and managed healthcare subindustries have the highest data exposure scores in the Sustainalytics subindustry universe. By contrast, the trucking, trading and distribution, toys and sporting goods, tobacco, and tires subindustries are among the subindustries with the lowest data exposure scores.

Exhibit 2 Subindustries With High Data Exposure Scores Are Lucrative Targets for Bad Actors



Source: Morningstar Sustainalytics.
Note: This chart excludes subindustries with data exposure scores of zero. Higher scores equal higher data exposure.

Not All Data Is Created Equal; Why Sensitivity Matters

While all personal information is considered "sensitive," the degree of data sensitivity and the ramifications of a data leak lie on a spectrum. Data sensitivity reflects the type of personal information typically processed, and varies by value, associated regulatory exposure and mandated protections, perceived social stigma, and the magnitude of fines, penalties, and reputational risk. All else equal, we would expect a breach of more sensitive information such as health records or social identification documents to lead to steeper fines and greater reputational damage, relative to less sensitive or publicly available information such as phone numbers or email addresses. (We discuss the impact of data sensitivity in more detail below, see "Regulatory Scrutiny.") To illustrate this, research by IBM/Ponemon[8] indicates that the healthcare and financial services industries that typically deal with the most sensitive personal information consistently have the highest cost of a data breach.

To estimate data sensitivity scores at a subindustry level, we built our proprietary data set with reference to five key types of personal information informed by various privacy laws and industry standards. In order of least to most sensitive, these categories are:

1. Basic consumer information including email addresses and phone numbers.
2. Financial information including credit card numbers.
3. Social identification documents including passports.
4. Personal health information.
5. Special categories of data (this category is drawn from the GDPR and CCPA and includes a person's race, political views, religious affiliation, or sexual orientation, among others).

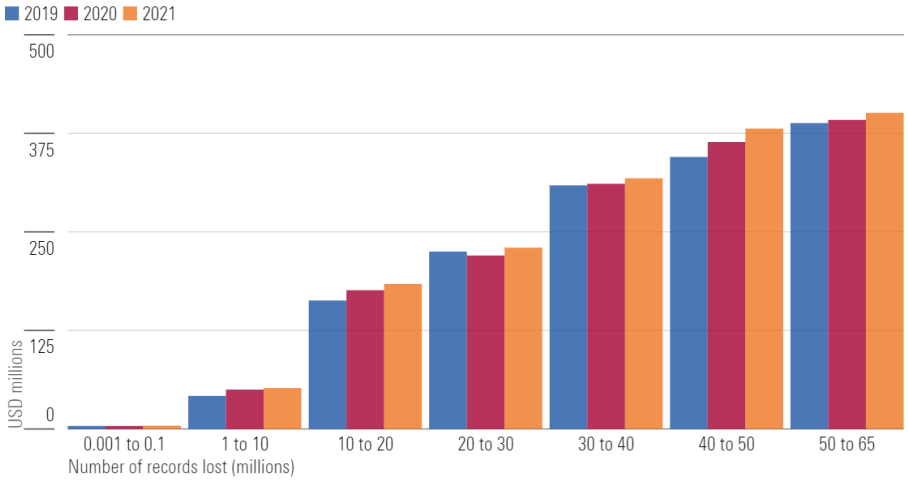
Based on industry consensus and our own estimates, we have established which of the five data categories are likely processed within a given subindustry as part of the normal course of business and then weighted these by the relative sensitivity to establish a data sensitivity score.

Bigger Is Typically Better in the Eyes of Hackers but Not for Targets

Data intensity reflects the volume of customer data typically processed by a subindustry as part of normal operations. All else equal, data-intensive subindustries are subject to significant data leakage risk and offer an attractive target for hackers. According to industry studies, the total cost of a data breach has a positive correlation with the number of compromised records. To illustrate this, research by IBM/Ponemon Institute in 2021 indicated that data breaches with 50 million to 65 million records were nearly 100 times more expensive than breaches with 1,000 to 100,000 records, as seen in Exhibit 3.

8 https://www.ibm.com/security/data-breach

Exhibit 3 All Else Equal, the Higher the Volume of Data Records Leaked, the Higher the Expected Cost



Source: IBM/Ponemon reports 2019, 2020 and 2021.
Note: Chart depicts the average total cost of a breach by number of records lost. The cost for breaches with over 1 million records lost is estimated using Monte Carlo simulation due to a small sample size. Estimated costs include both direct expenses such as detection measures and customer remediation, and indirect costs such as lost business. These estimates reflect costs only relevant to the data breach and not other potential impacts of DP&S risk, including ransomware attacks or penalties related to unlawful data use or disclosure.

We measure data intensity by estimating the number of personal information data points collected per customer within a subindustry. To do this, we again reference our proprietary data set to estimate the number of data categories collected per customer. While the absolute volume of data collected and associated risk will vary depending on the size of the respective company's customer base, our metric aims to identify subindustries that typically collect large volumes of data in the normal course of business.

Companies Operating a B2C Model Face Increased Accountability

Companies operating a business to consumer, or B2C, model or segment face a higher regulatory risk and compliance burden as they are held accountable for safeguarding customers' personal information, even if the processing is outsourced to third parties.

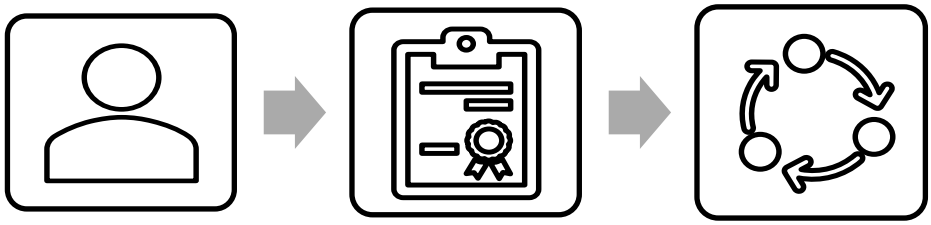
B2C companies—or those that provide some degree of B2C goods or services—are considered data controllers under the law and, increasingly, under privacy regulation (for example, the GDPR).[9] These companies—often found in the retail, healthcare, and banking subindustries—collect information directly from consumers and are accountable for its processing. Take banks, for example. They have significant direct contact with customers as well as large customer bases, with some of the largest diversified banks having tens of millions of individual customers globally. As part of their day-to-day business, they open and manage accounts for customers, process financial transactions, and offer products such as mortgages and auto loans. In the process, they collect data such as name, address,

9 We are abstracting from the legal complexity of data controllers and data processors. For example, we acknowledge that all companies are data controllers with respect to their employees.

social identification numbers, source and amount of income, account balances, and the like, to carry out business for their customers.

Among other things, data controllers have primary legal accountability with respect to the PII they process whether or not they process it themselves or contract these services to a third party. Controllers are also required to implement specific administrative and operational controls, such as privacy notices and data subject access rights. The third parties referred to above are known as data processors (often referred to as "service providers")—often found in enterprise software and services, research and consulting, and commercial services subindustries, among others—and are subject to much less privacy oversight. We depict the relationship between the data subject, data controller, and data processor in Exhibit 4.

Exhibit 4 Data Controllers Bear Higher Accountability for Safeguarding Customer Data



Customer/Data Subject—The individual whose data is being collected and processed	Business/Data Controller—Determines the purpose for which and how a customer's personal data is processed, and is accountable for lawful use and safeguarding	Business/Data Processor—Processes a customer's personal data on behalf of the controller

Source: Morningstar, European Union.

To provide a concrete example, in one of the more unlikely and costly breaches in the past 10 years, the payment accounts of one of the U.S.' largest retailers, Target, were breached. The cost of the breach sat at USD 202 million as of 2017, with further lawsuits pending[10]. However, the cause of the breach was its heating, ventilation, and air conditioning, or HVAC, vendor, which failed to keep its own operations secure. In short, the hackers used their access to the third-party HVAC provider to hack into Target's own network, and Target paid the price. This is a very common scenario.

Our analysis indicates that 54 subindustries have B2C operations, or 39% out of a total of 138 Sustainalytics subindustries. We have taken a conservative approach when assessing exposure by including subindustries whose constituent companies derive even a minority of revenue from B2C operations. Some of these are more intuitive, such as retailing, healthcare, and financial services; whereas others, such as data processing and REITs, have lower, yet sufficient risk exposure in our

10 https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031

opinion to flag. For example, constituents of the data processing subindustry such as Dropbox and PayPal act as both a data controller and data processor depending on the product or service offered.

Surveillance: The Controversial Yet Legal Practice

The surveillance risk driver refers to a government's propensity to surveil individual customers, along with industries perceived to be exposed to this type of surveillance. In this case, surveillance may include activities such as wiretapping and requests for access to personal data. While surveillance may be lawful, this controversial practice can have negative reputational and financial impacts on companies. For instance, subindustries most exposed to this risk driver such as internet software and services and telecommunication services face public and regulatory scrutiny for the actual or perceived surveillance activities of governments.

This issue came to the fore with the disclosure of the U.S. government's collection of telephony metadata under the Patriot Act, as well as with related controversies around Foreign Intelligence Surveillance Act warrants (and other country equivalents). This has led to the advent and increase in the disclosure of transparency reports by large companies that focus on government requests for company data, both received and fulfilled.

A recent example of potential surveillance activity has come to light during the debate by the U.S. Supreme Court regarding *Roe v. Wade*. As highlighted by the *Financial Times*,[11] local governments—particularly those in states with anti-abortion stances—may be able to obtain and use personal data to incriminate women seeking abortions. For instance, apps tracking menstrual cycles may collect this data and sell it to data brokers (discussed in detail below), who in turn can sell it to law enforcement, or whomever else is willing to pay for it. Such apps provide an avenue where highly personal data may easily, and even legally, be obtained by the government to carry out its own agenda. The trail of data from private companies to data brokers to government makes it possible for companies, institutions, and even the general public to gain access to intimate details of an individual's daily life and monitor their movements and decisions.

The topic of surveillance is an important and emerging risk, especially as more data is collected for every additional digital product and service used. However, in our view, for the time being, only two subindustries are directly exposed to this risk due to public perception of past practices, namely internet software and services, and telecommunication services. It is notable that other industries face early signs of similar exposure—for example, some financial institutions have begun to release transparency reports, but this has not yet led to broad public concerns about surveillance.

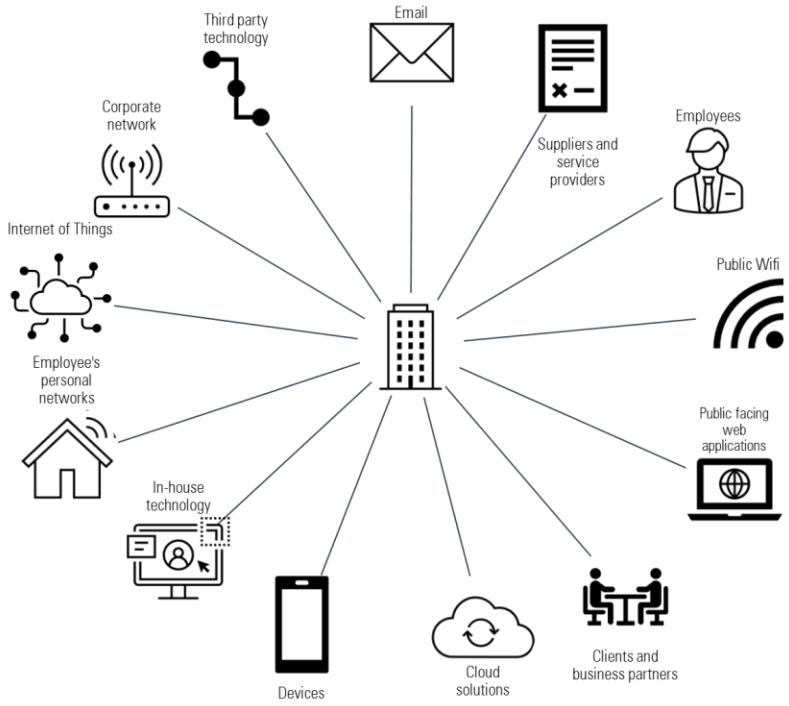
Digitizing and Outsourcing Create a Double-Edged Sword

In our framework, the attack surface reflects the degree of a subindustry's vulnerability to attack via technical infrastructure or a third-party supply chain. The larger the attack surface of a company, the more points of entry bad actors have to steal customer data or cause operational disruption through malicious activities.

11 https://www.ft.com/content/5f45a4e0-d9c0-4dbf-a1c7-bd86cfd0f605

A subindustry's vulnerability to attack is driven by its dependency on data, its exposure to the internet, and the complexity of its data management and information technology, or IT, systems, vendors, and partners. We also consider the standard service-provider supply chain within this dimension—when companies outsource activities that involve granting third-parties access to PII, they are increasing their attack surface with respect to that data. An increased attack surface increases the risk of hacking, malware, phishing, or other types of cyber security attacks. Exhibit 5 depicts the myriad of ways bad actors could gain access to the digital assets and networks of a company with interconnected, digitized operations.

Exhibit 5 Bad Actors Can Exploit an Increasing Array of Entry Points Into a Company



Source: Morningstar.

Attack Surface Is Driven by the Level of Digitization, Openness to the Internet, and Supply Chain

All things equal, the greater the degree of digitization, the higher the DP&S risk. This dimension of risk also includes what we call the "digital supply chain," namely technology that a company purchases or licenses from a third party, which in turn makes it vulnerable to a supply chain attack, such as the notorious SolarWinds hack in 2020.

Several metrics can be analyzed to assess a company's level of digitization. At a subindustry level, we find McKinsey's Industry Digitization Index[12] to offer the most comprehensive view, including two main factors: digital assets and digital usage.

Digital assets reflect the degree of a subindustry's investment in hardware, software, data solutions, and IT services. This includes traditional digital assets as well as investments in Internet of Things, big data/artificial intelligence solutions, and the operational technology, or OT, that controls physical processes. For our purposes, this factor may also serve as a proxy for digital supply chain. McKinsey's research indicates the highest digital asset scores are in information and communications technology, or ICT, and the lowest in agriculture and hunting.

Digital usage reflects the degree to which companies interact digitally with customers and suppliers, including interactions and financial transactions, the use of e-commerce platforms, and integrated social media. For our purposes, this factor is also a proxy for "openness to the internet," which is a key vulnerability and vector for cyberattacks. McKinsey's research indicates the highest digital usage scores are in ICT, media, professional services, and financial and insurance services.

During the COVID-19 pandemic, many industries were forced to undergo accelerated digitization, which increased their attack surface and DP&S risk profile. An example of this was highlighted by the *Financial Times*,[13] which reported that hospitality businesses are increasingly attractive targets for hackers as more processes—including customer interactions previously occurring face to face and customer data collection—were digitized during the pandemic. Hotels collect a rich set of customer data in high volumes, including contact details, passport information, and increasingly, health information, making them a natural, and now more accessible, target for bad actors. While we expect industries that experienced accelerated digitization during the pandemic can reap benefits, including potential operational efficiencies and greater flexibility, they will simultaneously face greater DP&S risk and now must invest to protect digital assets.

Critical Infrastructure Is an Attractive Target for Malicious Actors

Certain subindustries have innate characteristics that increase DP&S risk, namely their identification by national governments as "critical infrastructure," or CI. CI consists of sectors that have been identified as essential to the functioning of the economy and state. Each of these sectors is subject to what is often referred to as "critical infrastructure protection" that reflects their strategic and prestige value to bad actors wishing to cause disruption and malicious activity. However, there is no international consensus on what constitutes CI—it is a national prerogative. For example, the U.S. identifies 16 sectors that constitute CI, while the U.K. has 13.

12 https://www.mckinsey.com/~/media/mckinsey/industries/technology%20media%20and%20telecommunications/high%20tech/our%20insights/digital%20america%20a%20tale%20of%20the%20haves%20and%20have%20mores/mgi%20digital%20america_executive%20summary_december%202015.pdf

13 https://www.ft.com/content/347449f3-e620-4a5f-8735-0b7a824c2912

In our framework, we take a conservative approach and view each of the 16 U.S.-identified CI sectors (mapped to subindustries) as critical infrastructure, namely:

1. Chemical
2. Commercial facilities
3. Communications
4. Critical manufacturing
5. Dams
6. Defense industrial base
7. Emergency services
8. Energy
9. Financial services
10. Food and agriculture
11. Government facilities
12. Healthcare and public health
13. Information technology
14. Nuclear reactors, materials, and waste
15. Transportation systems
16. Water and wastewater systems

This is clearly an expansive list, and its explanatory power with respect to DP&S risk is diluted for our purposes. Accordingly, we rely more on the concept of "backbone critical infrastructure."

There is a greater global consensus on "backbone" critical infrastructure—the industries that are seen to form a single point of failure in an economy, typically including communications, utilities, energy, and transportation. The 2021 shutdown of the Colonial Pipeline was a game-changing attack on critical infrastructure: in May 2021, the company was subject to a ransomware attack—the largest cyberattack on oil infrastructure in U.S. history. This caused major economic disruption as the Colonial Pipeline provides the east coast of the U.S. with almost half its fuel supplies. Its closure led to flight cancellations, major fuel shortages, panic buying, and an increase in the cost of gas. The U.S. president even declared a state of emergency to prevent unsafe fuel transport practices.

Certain Drivers Are Best Assessed at a Company Level

In addition to the subindustry-level risk drivers identified above, we recommend investors consider two key drivers at a company level: the supply chain of service providers and involvement in data monetization. The breadth and depth of a company's supply chain—specifically, service providers that process or have access to personal information—present a significant risk. Second, companies that use personal data as a core product or service—data monetization—are also significantly exposed.

While these risk drivers are highly pertinent to assessing DP&S risk, we believe the assessment of exposure will be more appropriate when considering the unique structure and operations of a company, rather than at a subindustry level.

Increasing Scrutiny of Data Monetization Practices Threatens Business Models, Revenue Streams

Tangential to surveillance is the practice of using data as a core product or service, also known as data monetization. This business model heightens DP&S risk. We are observing increasing public concern over this issue, strong regulatory action that threatens associated business models, and disruptors like Apple actively undermining the ability of its Big Tech peers to leverage the necessary data through opt-out prompts.

We think it's important for investors to consider two types of data monetization: online behavioral advertising, or OBA, and data aggregation ("data brokers"). Put simply, OBA is targeted advertising based on a consumer profile that is generated using browsing behavior. This is achieved by tracking activity over time and across sites, using technologies such as cookies. These technologies are considered a form of profiling or even surveillance. OBA has become an increasing focus of privacy regulation (the GDPR and various "cookie laws," for example). Further, the EU's proposed Digital Services Act prescribes fines of up to 6% of global turnover for violations by tech platforms, which at a minimum include the major social media and search engine providers, including Meta's Facebook and Alphabet's Google.

Data aggregators (also known as data brokers) are companies that collect and aggregate data from public and private sources and then sell or license this data to other organizations. This data may include personal information ranging from basic demographics and purchase history to political affiliation and ethnicity. In short, data aggregators can provide detailed snapshots of an individual's data profile at various levels of depth and breadth, without the individual's knowledge (see the discussion of *Roe v. Wade* and menstrual tracking apps, above). Data brokers have been the subject of intense interest over the past five years, particularly with the passage of the GDPR, the Facebook-Cambridge Analytica scandal, and the passage of the CCPA. The CCPA specifically requires data brokers to publicly register with authorities to regulate the purchase and sale of personal data.[14]

Despite operating within the bounds of the law at present, we expect greater consumer awareness of data monetization could lead to reputational damage—particularly outside the usual suspects like social media. For instance, a recent report[15] by Human Rights Watch flagged concerns about education technology providers (which became vital in supporting remote learning during the COVID-19 pandemic) tracking student behavior inside and outside virtual classrooms. This included collecting data on their identity, location, and close contacts, at times without parental consent. More alarmingly, these providers often granted access to advertising companies that could leverage the data to inform behavioral advertising. Beyond the inherent infringement on children's privacy rights, this example illustrates how pervasive data monetization practices can be, and within products that consumers are arguably less likely to question.

14 The draft Regulations to the CCPA/CPRA include additional requirements but have not been settled at this time.
15 https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

Vulnerabilities in a Supply Chain Elevate DP&S Risk

Finally, investors should consider the standard service-provider supply chain—companies outsourcing activities that involve granting third parties access to PII increase their attack surface with respect to that data. A company's supply chain generates both efficiencies and vulnerabilities. We discuss this issue briefly under "Business to Consumer Operations," differentiating data controllers and data processors. Reiterating an example here, a bank may outsource check processing to one service provider and document destruction to another. The bank is accountable for the PII processed by these service providers and in case of incident or breach, will bear the cost of that accountability.

Regulatory Scrutiny of DP&S Issues Is Increasing in Breadth and Severity

Key considerations for companies facing high data privacy and security risks are the evolving regulatory landscape, the initial and ongoing compliance costs, and associated financial penalties for noncompliance. Over the past decade, data volume and digitization have increased rapidly, as have incident frequency and severity, along with associated costs. While regulatory risk varies across industry and jurisdiction, we are starting to see general strengthening and convergence in regulatory approach, at least within the developed world. The GDPR and CCPA are just the most recent and comprehensive of these developments. We have also begun to see significant developments related to free-standing cybersecurity law, technology design requirements, and increasing attention to critical infrastructure standards, a trend that has only accelerated with the SolarWinds and Colonial Pipeline attacks. According to the Forbes Technology Council, it is expected that by 2023, 65% of the world's population will have its personal information covered under modern privacy regulations, up from 10% in 2020. Although data breaches are only one component of data privacy and security risk, the most significant driver of delta in the cost of breaches is regulatory compliance.[16]

The degree of regulatory scrutiny typically correlates with the type of data processed. For example, personal health information is subject to more expansive and stringent privacy laws. All else equal, subindustries that are subject to more rigorous laws tend to incur higher operational and compliance costs related to both privacy and cybersecurity safeguards, and greater scrutiny around appropriate data use and antitrust. For example, even in the absence of omnibus privacy legislation, financial institutions are subject to what could be referred to as "privacy-adjacent" regulation, such as the Fair Credit Reporting Act, and the Privacy and Safeguards Rules under the Gramm-Leach-Bliley Act.

Further, it appears privacy issues are increasingly falling within the scope of antitrust agencies responsible for upholding consumer rights. Some of the largest privacy-related actions in the U.S. are initiated under consumer protection laws, such as the FTC Act, most notably the USD 5 billion Facebook settlement discussed in more detail above. Relatedly, the FTC has recently and repeatedly brought antitrust actions against major online platforms, including Facebook and Alphabet.[17]

Amid evolving regulation and the growing frequency and severity of financial penalties for noncompliance, companies are facing higher operational and compliance burdens as they prepare for

16 https://www.ibm.com/security/data-breach
17 https://www.forbes.com/advisor/investing/update-facebook-antitrust-lawsuit/

more onerous privacy and security regulation. As a result, companies are being forced to reassess internal protocols, undertake data mapping exercises to understand exposure, and realign practices for collecting, storing, and using customer data to ensure compliance with the most rigorous regulatory guidelines.

At the extreme, regulatory scrutiny of data monetization practices could threaten entire business models such as that of data brokers and primary—or at least high-margin—revenue streams for Big Tech providers such as Meta Platforms, Alphabet, and Amazon. We have observed increasingly severe penalties under GDPR for companies leveraging tracking technologies to collect customer data and inform targeted advertising, and for a lack of transparency with customers on how their data is being used. Moreover, as mentioned above, the proposed EU Digital Services Act, targets tech platforms with financial penalties of up to 6% of annual turnover for violations. Its counterpart, the Digital Markets Act, would see Big Tech "gatekeepers" subject to fines of up to 10% of global turnover for data-related anticompetitive behavior. While it is yet to be seen how far regulators will go to curb controversial collection and use of customer data, we expect the enforcement of existing legislation to continue to gather pace and new legislation to converge at a higher level of scrutiny.

What Is the Financial Materiality of DP&S Risk, and How Can It Be Mitigated?

The potential financial and reputational costs of data privacy and security risk are far reaching but can be mitigated through company-level management and competitive positioning. In the event of a data leak, perceived misuse, or cybersecurity attack, a company could expect to face financial penalties, regulatory action, reputational damage and lost business, and increased expenditure to upgrade software, infrastructure, and personnel, provide customer remediation, and strengthen detection and response measures. We also expect increasing societal and regulatory scrutiny of controversial data use, such as behavioral advertising, could lead to reputational damage or the destruction of high-margin revenue streams.

Notably, the cyber insurance industry is flagging concerns with increasing risk profiles, leading to higher premiums, decreasing coverage, and the exclusion of whole industries. Research firm Marsh & McLennan cites an inflection point in the market comparable to that faced by property insurers following Hurricane Andrew 30 years ago. In 2021, loss ratios neared 100%, premiums have more than doubled, and increased underwriting scrutiny has led to significant reductions in coverage. Moreover, coverage availability is now tied closely to implementing best-in-class security safeguards.[18] [19]

While there is evidentially a broad range of potential financial impacts stemming from DP&S risk, we believe investors need to consider both company-level risk mitigation as well as the company's competitive position when assessing financial materiality. Structural factors such as high customer switching costs or network effects may make it easier for a company to pass on costs or reduce customer attrition following a DP&S incident. Management teams can also take steps to minimize risk exposure at a company level through practices such as board- and executive-level risk oversight, regular

18 https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html
19 https://www.ft.com/content/60ddc050-a846-461a-aa10-5aaabf6b35a5

employee training, external audits, refraining from controversial data use and collection, and maintaining robust controls.

Competitive Positioning and Company Management Can Lessen Financial Materiality of DP&S Risk

When assessing the financial materiality of DP&S risk, Morningstar Equity Research encourages investors to consider how the competitive positioning of a company (which can be screened using the Economic Moat rating) can reduce financial impact. To illustrate this, while research from a 2020 McKinsey study[20] indicates that most consumers would not engage with, or cease to engage with, a company with concerning privacy and security practices, case studies from providers such as wide-moat Adobe and Meta Platforms suggest there are other factors at play.

We believe Adobe's high customer switching costs and network effect moat sources have created a shield limiting the financial impacts of DP&S risk. Adobe core products, including image editing software Photoshop, are industry standard and deeply ingrained for creative design professionals, leading to significant incentive to deploy and continue to use the products. Despite suffering multiple data breaches (resulting in an immaterial financial penalty), the company has been able to achieve healthy long-term customer and net income growth, which we think indicates the utility users reap from the products, and the burden of switching providers outweighs concerns about the privacy of their personal data, particularly when it is at the lower end of the sensitivity spectrum. Pleasingly, while Adobe, as a constituent of the enterprise and infrastructure software subindustry, faces high exposure to DP&S risk at a subindustry level, Sustainalytics data shows that strong company management has reduced the risk profile.

However, Sustainalytics takes a more pessimistic long-term view relative to Morningstar Equity Research on Meta Platforms. The company has an ESG Risk Rating of high, due in part to the severe risk assigned to its DP&S issue. Sustainalytics flags concerns about past regulatory penalties, ongoing and simultaneous investigations in multiple jurisdictions, emerging legislation, and controversy-laden media coverage. This may ultimately come to undermine the company's ability to rely on its current data monetization model. Sustainalytics views the company's current management of this risk as average.

Nonetheless, Morningstar Equity Research expects that Meta Platform's network effect moat source has supported the company's ability to achieve continued user base growth and maintain user engagement despite its high-profile DP&S issues. This network effect serves to both create barriers to success for new social network upstarts as well as barriers to exit for existing users who might leave behind friends, contacts, pictures, memories, and more by departing to alternative platforms. Morningstar Equity Research also believes that Meta's network effect moat source should help the company maintain healthy engagement levels from its massive user base of over 3.6 billion users. In turn, this will continue to attract demand from advertisers (the company's core revenue source) seeking a captive audience

20 https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20consumer%20data%20opportunity%20and%20the%20privacy%20imperative/The-consumer-data-opportunity-and-the-privacy-imperative.pdf

even if the ability to target users directly is diminished due to tighter regulation and Apple's tracking technology policies. We discuss this in further detail, as well Meta's investments in advertising technologies that workaround restrictions on user level tracking in our company report, "Meta's Advertising Business Will Turn Around," published May 18, 2022.

Separately, investors should consider other ways companies can mitigate subindustry-level exposure. For data privacy and security risk, a company can simplify complex systems or increase automation, strengthen access controls, run disaster recovery tests, and establish robust governance and oversight frameworks. In addition, Big Tech companies in particular have aggressively lobbied regulators, while also proactively front-running more onerous regulation through product innovation and simultaneously trying to differentiate themselves while hurting peers' ability to monetize customer data.

Finding Investment Opportunities Using a DP&S Lens

We have presented a framework for investors to consider the key drivers of DP&S risk, how this risk could materialize, and how companies can mitigate the risk at the company level. With those factors in mind, here are two potential strategies to play the DP&S theme:

1. Cheap, negligible DP&S risk, and moaty stocks: Stocks rated 5-stars with moats facing relatively lower exposure to data privacy and security risk (Exhibit 6).

2. Cheap stocks with high or severe DP&S risk at a subindustry level but average to strong management indicators: Companies screened by Sustainalytics as having average to strong management practices to mitigate systematic risk (Exhibit 7).

Exhibit 6 Undervalued, Moaty Stocks With Negligible DP&S Risk Exposure

Company	Ticker	Morningstar Rating	Currency	Current Price	Fair Value	Price/Fair Value	Market Cap (USD). Bb)	Moat	Uncertainty	Sustainalytics Subindustry
Adient	NYS:ADNT	★★★★★	USD	31	64	0.49	3.0	Narrow	Very High	Auto Parts
AkzoNobel	AMS:AKZA	★★★★★	EUR	62	107	0.58	12.1	Narrow	Medium	Specialty Chemicals
Alstom	PAR:ALO	★★★★★	EUR	23	38	0.61	9.4	Narrow	Medium	Heavy Machinery and Trucks
Anheuser-Busch InBev	BRU:ABI	★★★★★	EUR	50	80	0.62	90.6	Wide	Medium	Beer, Wine and Spirits
Ansell	ASX:ANN	★★★★★	AUD	21	32	0.68	1.9	Narrow	Low	Medical Supplies
BASF	ETR:BAS	★★★★★	EUR	41	66	0.63	42.0	Narrow	Medium	Diversified Chemicals
Blue Moon International	HKG:06993	★★★★★	HKD	6	11	0.61	4.8	Narrow	Medium	Household Products
BMW Group	ETR:BMW	★★★★★	EUR	75	146	0.51	54.0	Narrow	High	Automobiles
BorgWarner	NYS:BWA	★★★★★	USD	35	73	0.48	8.5	Narrow	High	Auto Parts
Boston Beer Co	NYS:SAM	★★★★★	USD	330	740	0.45	3.8	Narrow	Medium	Beer, Wine and Spirits
Compass Minerals	NYS:CMP	★★★★★	USD	36	85	0.42	1.2	Wide	High	Diversified Metals Mining
Continental	ETR:CON	★★★★★	EUR	67	143	0.47	14.9	Narrow	High	Auto Parts
Crane Company	NYS:CR	★★★★★	USD	85	126	0.67	4.8	Narrow	Medium	Industrial Machinery
Discovery	NAS:WBD	★★★★★	USD	14	40	0.35	33.9	Narrow	High	Non-Residential Construction
DuPont de Nemours	NYS:DD	★★★★★	USD	55	100	0.55	28.4	Narrow	Medium	Specialty Chemicals
Eastman Chemical Company	NYS:EMN	★★★★★	USD	86	140	0.62	11.5	Narrow	Medium	Diversified Chemicals
Equitrans Midstream	NYS:ETRN	★★★★★	USD	6	14	0.45	2.8	Narrow	High	Oil & Gas Storage and Transportation
Fortive	NYS:FTV	★★★★★	USD	55	85	0.64	19.5	Narrow	Medium	Conglomerates
Fortune Brands Home & Security	NYS:FBHS	★★★★★	USD	61	99	0.62	7.7	Narrow	Medium	Building Products
General Electric	NYS:GE	★★★★★	USD	64	126	0.51	71.0	Narrow	High	Conglomerates
Harmonic Drive Systems	TKS:6324	★★★★★	JPY	3,115	6,400	0.49	2.2	Wide	High	Industrial Machinery
Imperial Brands	LON:IMB	★★★★★	GBX	1,817	2,900	0.63	21.4	Wide	Medium	Tobacco
Itt	NYS:ITT	★★★★★	USD	66	100	0.66	5.6	Narrow	Medium	Industrial Machinery
Jungheinrich	DUS:JUN3	★★★★★	EUR	22	36	0.61	2.5	Narrow	Medium	Industrial Machinery
KION Group	ETR:KGX	★★★★★	EUR	39	80	0.48	5.6	Narrow	Medium	Industrial Machinery
Kone	HEL:KNEBV	★★★★★	EUR	43	56	0.76	24.4	Wide	Low	Industrial Machinery
Malibu Boats	NAS:MBUU	★★★★★	USD	54	100	0.54	1.1	Narrow	High	Toys and Sporting Goods
Masco	NYS:MAS	★★★★★	USD	50	75	0.66	11.2	Wide	Medium	Building Products
Polaris Industries	NYS:PII	★★★★★	USD	104	175	0.60	6.1	Wide	High	Toys and Sporting Goods
Schindler Holding	SWX:SCHN	★★★★★	CHF	162	225	0.72	18.7	Wide	Low	Industrial Machinery
Shenzhou International	HKG:02313	★★★★★	HKD	91	171	0.53	17.5	Narrow	Medium	Textiles
The a2 Milk Company	ASX:A2M	★★★★★	AUD	4	8	0.59	2.2	Narrow	High	Packaged Foods
WESCO International	NYS:WCC	★★★★★	USD	104	168	0.62	5.3	Narrow	Medium	Trading and Distribution
Zhengzhou Yutong Bus Company	SHG:600066	★★★★★	CNY	9	17	0.54	3.0	Narrow	Medium	Heavy Machinery and Trucks

Source: Morningstar and Sustainalytics, as of 06/24/2022.

Exhibit 7 Cheap Stocks With High or Severe DP&S Risk, but Average to Strong Company Level Management

Company	Ticker	Morningstar Rating	Currency	Current Price	Fair Value	Price/Fair Value	Market Cap (USD). Bb)	Moat	Uncertainty	Sustainalytics Subindustry
Admiral Group	LON:ADM	★★★★★	GBX	2,172	3,500	0.62	8.0	Narrow	Medium	Property and Casualty Insurance
AUB Group	ASX:AUB	★★★★★	AUD	18	28	0.64	1.1	Narrow	Medium	Insurance Brokers
Comcast	NAS:CMCSA	★★★★★	USD	39	60	0.65	174.3	Wide	Medium	Telecommunication Services
Delivery Hero	ETR:DHER	★★★★★	EUR	38	97	0.39	9.3	Narrow	High	Internet Software and Services
DoorDash	NYS:DASH	★★★★★	USD	70	163	0.43	22.9	Narrow	Very High	Internet Software and Services
eBay	NAS:EBAY	★★★★★	USD	43	65	0.66	24.1	Narrow	Medium	Internet Software and Services
Fastly	NYS:FSLY	★★★★★	USD	13	25	0.51	1.4	None	Very High	Internet Software and Services
Just Eat Takeaway.com	AMS:TKWY	★★★★★	EUR	18	126	0.14	3.9	Narrow	High	Internet Software and Services
Lyft	NAS:LYFT	★★★★★	USD	16	65	0.24	5.2	Narrow	Very High	Internet Software and Services
Megaport	ASX:MP1	★★★★★	AUD	5	15	0.37	0.5	None	Very High	Internet Software and Services
MercadoLibre	NAS:MELI	★★★★★	USD	699	1,570	0.45	34.1	Wide	High	Internet Software and Services
Millicom International Cellular	NAS:TIGO	★★★★★	USD	15	34	0.44	2.0	Narrow	High	Telecommunication Services
Pinterest	NYS:PINS	★★★★★	USD	20	48	0.41	12.5	Narrow	Very High	Internet Software and Services
Prudential UK	LON:PRU	★★★★★	GBX	935	1,480	0.63	31.5	None	Medium	Life and Health Insurance
Rakuten (Internet Retail)	TKS:4755	★★★★★	JPY	616	1,300	0.47	7.2	Narrow	Very High	Internet Software and Services
Snap Group	NYS:SNAP	★★★★★	USD	14	49	0.28	21.4	None	Very High	Internet Software and Services
Tencent Holdings	HKG:00700	★★★★★	HKD	375	741	0.51	459.7	Wide	High	Internet Software and Services
Tencent Music Entertainment Group	NYS:TME	★★★★★	USD	5	8	0.60	8.2	Narrow	High	Internet Software and Services
Twilio	NYS:TWLO	★★★★★	USD	97	300	0.32	16.1	Narrow	Very High	Internet Software and Services
Uber	NYS:UBER	★★★★★	USD	22	73	0.31	42.2	Narrow	Very High	Internet Software and Services

Source: Morningstar and Sustainalytics, as of 06/24/2022.

Within these lists, there are several names we'd call out:

Anheuser-Busch InBev, Imperial Brands, and Polaris

Beer, wine and spirits, tobacco, and toys and sporting goods are subindustries that face negligible data privacy and security risk, in our opinion. The primary DP&S risk driver for these subindustries is modest exposure to digitization.

For investors seeking undervalued opportunities with low DP&S risk, we see meaningful discounts to our fair value estimates for Anheuser-Busch In Bev, Imperial Brands, and Polaris. All companies enjoy wide moat ratings and trade in 5-star territory.

Anheuser-Busch InBev, or AB InBev, has proven resilient amid the current inflationary environment, with consumers willing to accept higher prices in most regions without material impact on demand. AB InBev is well placed with strong emerging market exposure and a cost advantage in some of its scaled regions. We believe the market is undervaluing this opportunity, and the company should be trading at multiples of normalized earnings at least in line with competitors. We expect the share price to converge toward our fair value estimate as balance sheet leverage is reduced.

Imperial Brands has been executing well on operational and financial improvement, with stabilizing volume trends and market share in the company's core markets following sizable declines in recent years. We expect Imperial can achieve flat revenue over the next five years if the company balances its structural cigarette volume decline with price increases and mitigates lower cigarette volumes with rising volumes from new products such as heated tobacco. The company boasts a high cash conversion rate, high dividend yield, and improving balance sheet, which suggests that shareholder returns could be significantly increased in coming years, including through potential share repurchases if the stock remains undervalued.

Powersport manufacturer Polaris continues to benefit from strong demand, and we expect recent profitability headwinds from inflation and supply chain issues to be transitionary. The company benefits from strong brand assets and low-cost production. We believe the market is undervaluing Polaris' unique position to benefit from the backfill of the dealer channel that has faced stock shortage and robust pre-orders. Even in the event of a normal duration recession, we expect manufacturing should fail to slow as restocking takes place.

Millicom International Cellular, Prudential UK, and Tencent

Telecommunications, insurance brokers, and internet software and services are subindustries with the highest data privacy and security risk, in our view. The risk exposure for these subindustries is primarily driven by data exposure, followed by business-to-consumer operating models and digitization.

While Millicom International Cellular, Prudential UK, and Tencent are constituents on these high DP&S risk subindustries, Sustainalytics data shows that these companies are minimizing their risk exposure through strong practices that cumulatively include board level risk oversight, regular employee training

and independent audits, policy commitments, and limiting data collection to only what is necessary for product function. At present, all three companies trade in 5-star territory, representing material risk adjusted upside potential for investors.

Investors Should Push for More DP&S Risk Data

Despite being an ESG issue of growing importance, access to reliable and consistent data to assess exposure at the company level is limited. Reasons for this include different DP&S incident reporting regimes, disincentives to report due to security concerns, lack of formalized reporting requirements, and even inconsistency in requirements from the regulators themselves. For instance, under current regulation, companies have significant discretion over how they classify what is either an "incident" or a "breach" and whether to report the event, making it challenging to compare the management of DP&S risk between companies. With scant disclosure, it is challenging to understand the root cause of events and where the greatest exposure to risk lies. Further, anecdotal evidence following the implementation of GDPR legislation implies that companies have struggled to map their internal data collection especially across varied IT infrastructure or third parties, let alone disclose this publicly.

We present a list of questions investors can ask company management and how to use this information to better understand DP&S risk. We also recommend investors supplement these questions by referencing the Sustainalytics ESG risk rating reports to understand the key risk exposures and company management.

Exhibit 8 Investors Can Use the Suggested Questions to Gain a Better Understanding of a Company's DP&S Risk

Suggested questions	Next steps
How many data subjects does your company collect and process data for? **How many unique data records does your company collect and process?** **What types of personal information do you collect during the normal course of business?** **What steps has your company taken to map data inventory (i.e. to understand what and where data is being collected, processed, and stored?)** **Does your company only collect data that is directly related to the product/service offered?**	Investors can utilize this information in combination with the IBM/Ponemon Institute's estimated cost per record lost to understand the potential financial implications from a data breach. While this is a useful proxy and starting point for investors, we encourage investors to also consider broader DP&S-related costs such ransom payments and costs associated with inappropriate or unlawful use or disclosure of data. In relation to this, investors should query the steps companies are taking to understand their own data exposure and what data will be collected going forward. It is considered best practice under leading data privacy regulation that companies limit data collection to only what is necessary for the product/service offered.
Is your company compliant with leading privacy regulation such as GDPR? **Is your company certified with the international standard for information security management (ISO 270001)? If not, have you documented and do you follow the suite of ISO 27001 information security procedures, or do you have commensurate policies in place?** **Can your company share a SOC 2 report (which provides assurance of the suitability and effectiveness of security and privacy controls)?** **Does your company have a privacy team with relevant certifications (e.g. Certified Information Privacy Professional qualification)?** **Does your company have a security team with relevant certifications (e.g. Certified Information Systems Security Professional, or Certified Information Systems Auditor qualifications)?** **Does your company's board exercise formal DP&S oversight with at least annual risk reviews?** **Does your company have at least one C-Suite executive responsible for privacy and security (e.g. chief information security officer or chief privacy officer)?**	Investors can consider the GDPR as a global benchmark for data privacy best practices. Investors can assess whether companies that fall under GDPR regulation are compliant and use the regulation as a yardstick to assess the practices of companies that are not directly covered by the regulation. Investors can use external qualifications and assessments, and internal appointments such as those listed here to gauge the robustness of a company's management and oversight of DP&S risk.

What steps does your company take to assess and manage risk related to third-party service providers? **In relation to this, how does your company protect against supply chain attacks?** **Does your company contractually require third parties to abide by industry standard DP&S safeguards?**	Investors can consider initial and ongoing due diligence screening of potential and existing contracted third parties as a reasonable measure for assessing supply chain risk. This may include onboarding questionnaires that assess a third party's own DP&S practices, including policies and infrastructure to safeguard customers' personal data. A lack of due diligence or DP&S practices by third parties that fall below the standard set by the contracting company may imply higher supply chain risk.
How many security incidents has your company had in the past five years, and what steps were taken to remediate and prevent the issues from reoccurring? **Was your company able to establish the root cause of the incident?** **What was the financial impact of these incidents, including regulatory fines, remediation costs, and lost business (if any)?** **Does your company have cyber insurance?** **If yes, what does this insurance cover, including amount of coverage and inclusions/exclusions?**	Investors can compare the frequency and financial cost of incidents to peers (where data is available) and to published industry data via providers such as IBM/Ponemon. Information on prevention measures and cyber insurance coverage may inform the probability and financial materiality of future incidents. If a company does not have cyber insurance, this is a concern. It may mean that the company has failed the cyber insurance due diligence process or is not properly managing the risk. Cyber insurance companies are now leveraging better actuarial data and doing deep due diligence on industry standard practices before approving insurance and setting insurance rates.
In what way (if any) is your company employing data monetization practices? **Does your company sell customer data to third parties including data brokers?**	If a company derives revenue from data monetization practices, investors should factor in potential regulatory and/or societal scrutiny that could lead to penalties or lower demand.

Source: Morningstar and Morningstar Sustainalytics.

Appendix

Our Proprietary Dataset

In light of data disclosure limitations, we have developed an exposure criteria dataset that informs estimated risk driver exposure scores for each of the Sustainalytics subindustries. This dataset was informed by industry expertise and consensus, keystone regulation, industry papers cited throughout the report, and consultation with relevant internal stakeholders. The dataset uses a combination of binary scoring for risk drivers such as data sensitivity and critical infrastructure (i.e. Is subindustry A likely to collect social identification numbers as part of normal operations, or not, or is this subindustry considered critical infrastructure, or not), and scale-based scoring for risk drivers such as digitization based on the cited McKinsey digitization index.

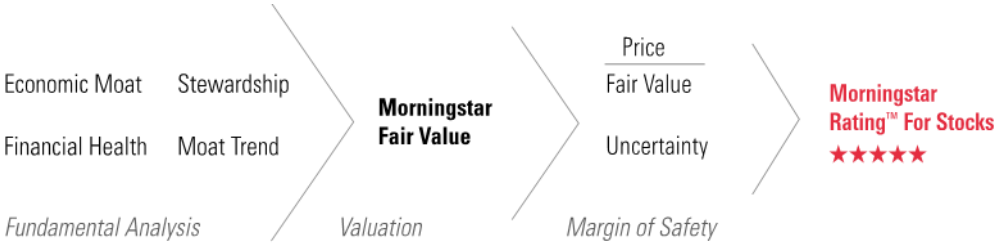
Research Methodology for Valuing Companies

Overview

At the heart of our valuation system is a detailed projection of a company's future cash flows, resulting from our analysts' research. Analysts create custom industry and company assumptions to feed income statement, balance sheet, and capital investment assumptions into our globally standardized, proprietary discounted cash flow, or DCF, modeling templates. We use scenario analysis, in-depth competitive advantage analysis, and a variety of other analytical tools to augment this process. Moreover, we think analyzing valuation through discounted cash flows presents a better lens for viewing cyclical companies, high-growth firms, businesses with finite lives (for example, mines), or companies expected to generate negative earnings over the next few years. That said, we don't dismiss multiples altogether but rather use them as supporting cross-checks for our DCF-based fair value estimates. We also acknowledge that DCF models offer their own challenges (including a potential proliferation of estimated inputs and the possibility that the method may miss short-term market-price movements), but we believe these negatives are mitigated by deep analysis and our long-term approach.

Morningstar's equity research group ("we," "our") believes that a company's intrinsic worth results from the future cash flows it can generate. The Morningstar Rating for stocks identifies stocks trading at a discount or premium to their intrinsic worth—or fair value estimate, in Morningstar terminology. Five-star stocks sell for the biggest risk-adjusted discount to their fair values, whereas 1-star stocks trade at premiums to their intrinsic worth.

Morningstar Research Methodology



Source: Morningstar.

Four key components drive the Morningstar rating: 1) our assessment of the firm's economic moat, 2) our estimate of the stock's fair value, 3) our uncertainty around that fair value estimate and 4) the current market price. This process ultimately culminates in our single-point star rating.

Economic Moat

The concept of an economic moat plays a vital role not only in our qualitative assessment of a firm's long-term investment potential, but also in the actual calculation of our fair value estimates. An economic moat is a structural feature that allows a firm to sustain excess profits over a long period of time. We define economic profits as returns on invested capital (or ROIC) over and above our estimate of a firm's cost of capital, or weighted average cost of capital (or WACC). Without a moat, profits are more susceptible to competition. We have identified five sources of economic moats: intangible assets, switching costs, network effect, cost advantage, and efficient scale.

Companies with a narrow moat are those we believe are more likely than not to achieve normalized excess returns for at least the next 10 years. Wide-moat companies are those in which we have very high confidence that excess returns will remain for 10 years, with excess returns more likely than not to remain for at least 20 years. The longer a firm generates economic profits, the higher its intrinsic value. We believe low-quality, no-moat companies will see their normalized returns gravitate toward the firm's cost of capital more quickly than companies with moats.

To assess the sustainability of excess profits, analysts perform ongoing assessments of the moat trend. A firm's moat trend is positive in cases where we think its sources of competitive advantage are growing stronger; stable where we don't anticipate changes to competitive advantages over the next several years; or negative when we see signs of deterioration.

Estimated Fair Value

Combining our analysts' financial forecasts with the firm's economic moat helps us assess how long returns on invested capital are likely to exceed the firm's cost of capital. Returns of firms with a wide economic moat rating are assumed to fade to the perpetuity

period over a longer period of time than the returns of narrow-moat firms, and both will fade slower than no-moat firms, increasing our estimate of their intrinsic value.

Our model is divided into three distinct stages:

Stage I: Explicit Forecast
In this stage, which can last five to 10 years, analysts make full financial statement forecasts, including items such as revenue, profit margins, tax rates, changes in working-capital accounts, and capital spending. Based on these projections, we calculate earnings before interest, after taxes, or EBI, and the net new investment, or NNI, to derive our annual free cash flow forecast.

Stage II: Fade
The second stage of our model is the period it will take the company's return on new invested capital—the return on capital of the next dollar invested, or RONIC—to decline (or rise) to its cost of capital. During the Stage II period, we use a formula to approximate cash flows in lieu of explicitly modeling the income statement, balance sheet, and cash flow statement as we do in Stage I. The length of the second stage depends on the strength of the company's economic moat. We forecast this period to last anywhere from one year (for companies with no economic moat) to 10–15 years or more (for wide-moat companies). During this period, cash flows are forecast using four assumptions: an average growth rate for EBI over the period, a normalized investment rate, average return on new invested capital (RONIC), and the number of years until perpetuity, when excess returns cease. The investment rate and return on new invested capital decline until a perpetuity value is calculated. In the case of firms that do not earn their cost of capital, we assume marginal ROICs rise to the firm's cost of capital (usually attributable to less reinvestment), and we may truncate the second stage.

Stage III: Perpetuity
Once a company's marginal ROIC hits its cost of capital, we calculate a continuing value, using a standard perpetuity formula. At perpetuity, we assume that any growth or decline or investment in the business neither creates nor destroys value and that any new investment provides a return in line with estimated WACC.

Because a dollar earned today is worth more than a dollar earned tomorrow, we discount our projections of cash flows in stages I, II, and III to arrive at a total present value of expected future cash flows. Because we are modeling free cash flow to the firm—representing cash available to provide a return to all capital providers—we discount future cash flows using the WACC, which is a weighted average of the costs of equity, debt, and preferred stock (and any other funding sources), using expected future proportionate long-term market-value weights.

Uncertainty Around That Fair Value Estimate
Morningstar's Uncertainty Rating captures a range of likely potential intrinsic values for a company and uses it to assign the margin of safety required before investing, which in turn explicitly drives our stock star rating system. The Uncertainty Rating represents the analysts' ability to bound the estimated value of the shares in a company around the Fair Value Estimate, based on the characteristics of the business underlying the stock, including operating and financial leverage, sales sensitivity to the overall economy, product concentration, pricing power, and other company-specific factors.

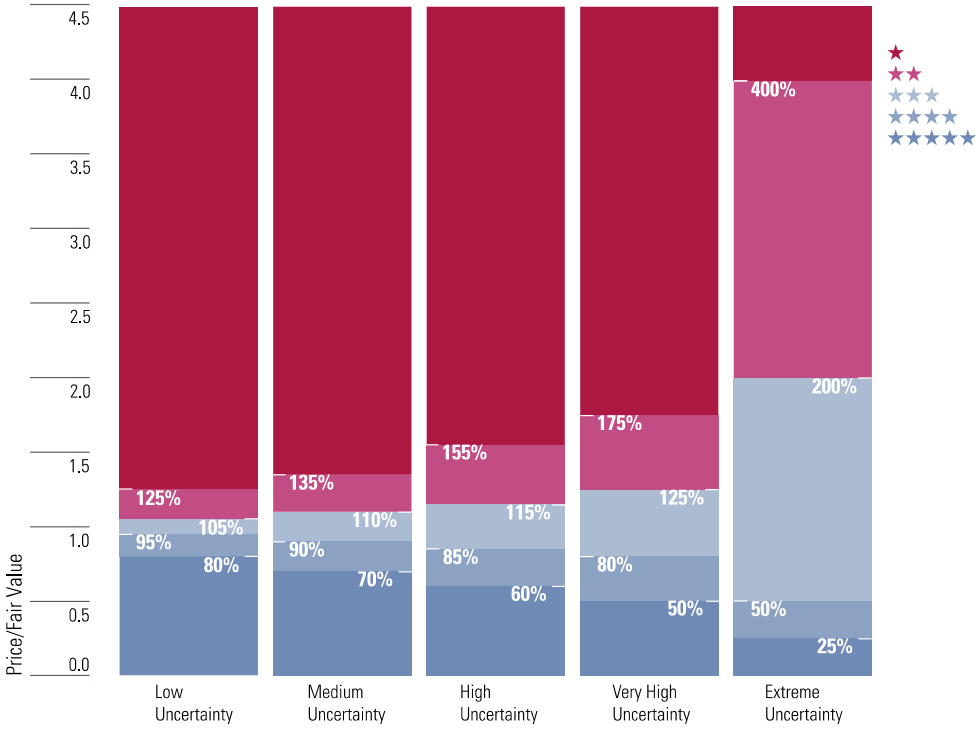
Analysts consider at least two scenarios in addition to their base case: a bull case and a bear case. Assumptions are chosen such that the analyst believes there is a 25% probability that the company will perform better than the bull case, and a 25% probability that the company will perform worse than the bear case. The distance between the bull and bear cases is an important indicator of the uncertainty underlying the fair value estimate.

Our recommended margin of safety widens as our uncertainty of the estimated value of the equity increases. The more uncertain we are about the estimated value of the equity, the greater the discount we require relative to our estimate of the value of the firm before we would recommend the purchase of the shares. In addition, the uncertainty rating provides guidance in portfolio construction based on risk tolerance.

Our uncertainty ratings for our qualitative analysis are low, medium, high, very high, and extreme.

- Low–margin of safety for 5-star rating is a 20% discount and for 1-star rating is 25% premium.
- Medium–margin of safety for 5-star rating is a 30% discount and for 1-star rating is 35% premium.
- High–margin of safety for 5-star rating is a 40% discount and for 1-star rating is 55% premium.
- Very High–margin of safety for 5-star rating is a 50% discount and for 1-star rating is 75% premium.
- Extreme– margin of safety for 5-star rating is a 75% discount and for 1-star rating is 300% premium.

Morningstar Equity Research Star Rating Methodology



Market Price

The market prices used in this analysis and noted in the report come from exchange on which the stock is listed which we believe is a reliable source.

For more details about our methodology, please go to https://shareholders.morningstar.com.

Morningstar Star Rating for Stocks

Once we determine the fair value estimate of a stock, we compare it with the stock's current market price on a daily basis, and the star rating is automatically re-calculated at the market close on every day the market on which the stock is listed is open. Our analysts keep close tabs on the companies they follow, and, based on thorough and ongoing analysis, raise or lower their fair value estimates as warranted.

Please note, there is no predefined distribution of stars. That is, the percentage of stocks that earn 5 stars can fluctuate daily, so the star ratings, in the aggregate, can serve as a gauge of the broader market's valuation. When there are many 5-star stocks, the stock market as a whole is more undervalued, in our opinion, than when very few companies garner our highest rating.

We expect that if our base-case assumptions are true the market price will converge on our fair value estimate over time, generally within three years (although it is impossible to predict the exact time frame in which market prices may adjust).

Our star ratings are guideposts to a broad audience and individuals must consider their own specific investment goals, risk tolerance, tax situation, time horizon, income needs, and complete investment portfolio, among other factors.

The Morningstar Star Ratings for stocks are defined below:

★★★★★ We believe appreciation beyond a fair risk-adjusted return is highly likely over a multiyear time frame. Scenario analysis developed by our analysts indicates that the current market price represents an excessively pessimistic outlook, limiting downside risk and maximizing upside potential.

★★★★ We believe appreciation beyond a fair risk-adjusted return is likely.

★★★ Indicates our belief that investors are likely to receive a fair risk-adjusted return (approximately cost of equity).

★★ We believe investors are likely to receive a less than fair risk-adjusted return.

★ Indicates a high probability of undesirable risk-adjusted returns from the current market price over a multiyear time frame, based on our analysis. Scenario analysis by our analysts indicates that the market is pricing in an excessively optimistic outlook, limiting upside potential and leaving the investor exposed to Capital loss.

Risk Warning
Please note that investments in securities are subject to market and other risks and there is no assurance or guarantee that the intended investment objectives will be achieved. Past performance of a security may or may not be sustained in future and is no indication of future performance. A security investment return and an investor's principal value will fluctuate so that, when redeemed, an investor's shares may be worth more or less than their original cost. A security's current investment performance may be lower or higher than the investment performance noted within the report. Morningstar's Uncertainty Rating serves as a useful data point with respect to sensitivity analysis of the assumptions used in our determining a fair value price.

General Disclosure

Unless otherwise provided in a separate agreement, recipients accessing this report may only use it in the country in which the Morningstar distributor is based. Unless stated otherwise, the original distributor of the report is Morningstar Research Services LLC, a U.S.A. domiciled financial institution.

This report is for informational purposes only and has no regard to the specific investment objectives, financial situation, or particular needs of any specific recipient. This publication is intended to provide information to assist institutional investors in making their own investment decisions, not to provide investment advice to any specific investor. Therefore, investments discussed and recommendations made herein may not be suitable for all investors; recipients must exercise their own independent judgment as to the suitability of such investments and recommendations in the light of their own investment objectives, experience, taxation status, and financial position.

The information, data, analyses, and opinions presented herein are not warranted to be accurate, correct, complete, or timely. Unless otherwise provided in a separate agreement, neither Morningstar, Inc. nor the Equity Research Group represents that the report contents meet all of the presentation and/or disclosure standards applicable in the jurisdiction the recipient is located.

Except as otherwise required by law or provided for in a separate agreement, the analyst, Morningstar, Inc. and the Equity Research Group and their officers, directors and employees shall not be responsible or liable for any trading decisions, damages or other losses resulting from, or related to, the information, data, analyses or opinions within the report. The Equity Research Group encourages recipients of this report to read all relevant issue documents for example, prospectus) pertaining to the security concerned, including without limitation, information relevant to its investment objectives, risks, and costs before making an investment decision and when deemed necessary, to seek the advice of a legal, tax, and/or accounting professional.

The Report and its contents are not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any locality, state, country, or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation or which would subject Morningstar, Inc. or its affiliates to any registration or licensing requirements in such jurisdiction.

Where this report is made available in a language other than English and in the case of inconsistencies between the English and translated versions of the report, the English version will control and supersede any ambiguities associated with any part or section of a report that has been issued in a foreign language. Neither the analyst, Morningstar, Inc., nor the Equity Research Group guarantees the accuracy of the translations.

This report may be distributed in certain localities, countries and/or jurisdictions ("Territories") by independent third parties or independent intermediaries and/or distributors ("Distributors"). Such Distributors are not acting as agents or representatives of the analyst, Morningstar, Inc. or the Equity Research Group. In Territories where a Distributor distributes our report, the Distributor is solely responsible for complying with all applicable regulations, laws, rules, circulars, codes, and guidelines established by local and/or regional regulatory bodies, including laws in connection with the distribution third-party research reports.

Conflicts of Interest

- No interests are held by the analyst with respect to the security subject of this investment research report.

  Morningstar, Inc. may hold a long position in the security subject of this investment research report that exceeds 0.5% of the total issued share capital of the security. To determine if such is the case, please click http://msi.morningstar.com and http://mdi.morningstar.com.

- Analysts' compensation is derived from Morningstar, Inc.'s overall earnings and consists of salary, bonus and in some cases restricted stock.

- Neither Morningstar, Inc. nor the Equity Research Group receives commissions for providing research nor do they charge companies to be rated.

- Neither Morningstar, Inc. nor the Equity Research Group is a market maker or a liquidity provider of the security noted within this report.

- Neither Morningstar, Inc. nor the Equity Research Group has been a lead manager or co-lead manager over the previous 12 months of any publicly disclosed offer of financial instruments of the issuer.

- Morningstar, Inc.'s investment management group does have arrangements with financial institutions to provide portfolio management/investment advice some of which an analyst may issue investment research reports on. However, analysts do not have authority over Morningstar's investment management group's business arrangements nor allow employees from the investment management group to participate or influence the analysis or opinion prepared by them.

- Morningstar, Inc. is a publicly traded company (Ticker Symbol: MORN) and thus a financial institution the security of which is the subject of this report may own more than 5% of Morningstar, Inc.'s total outstanding shares. Please access Morningstar, Inc.'s proxy statement, "Security Ownership of Certain Beneficial Owners and Management" section http://investorrelations.morningstar.com/sec.cfm?doctype=Proxy&year=&x=12

- Morningstar, Inc. may provide the product issuer or its related entities with services or products for a fee and on an arms' length basis including software products and licenses, research and consulting services, data services, licenses to republish our ratings and research in their promotional material, event sponsorship and website advertising.

  Further information on Morningstar, Inc.'s conflict of interest policies is available from http://global.morningstar.com/equitydisclosures. Also, please note analysts are subject to the CFA Institute's Code of Ethics and Standards of Professional Conduct.

  For a list of securities which the Equity Research Group currently covers and provides written analysis on please contact your local Morningstar office. In addition, for historical analysis of securities covered, including their fair value estimate, please contact your local office.

  For Recipients in Australia: This Report has been issued and distributed in Australia by Morningstar Australasia Pty. Ltd. (ABN: 95 090 665 544; ASFL: 240892). Morningstar Australasia Pty. Ltd. is the provider of the general advice ("the Service") and takes responsibility for the production of this report. The Service is provided through the research of investment products. To the extent the Report contains general advice it has been prepared without reference to an investor's objectives, financial situation or needs. Investors should consider the advice in light of these matters and, if applicable, the relevant Product Disclosure Statement before making any decision to invest. Refer to our Financial Services Guide, or FSG, for more information at http://www.morningstar.com.au/fsg.pdf.

  For Recipients in New Zealand: This report has been issued and distributed by Morningstar Australasia Pty Ltd and/or Morningstar Research Ltd (together 'Morningstar'). Morningstar is the provider of the regulated financial advice and takes

responsibility for the production of this report. To the extent the report contains regulated financial advice it has been prepared without reference to an investor's objectives, financial situation or needs. Investors should consider the advice in light of these matters and, if applicable, the relevant Product Disclosure Statement before making any decision to invest. Refer to our Financial Advice Provider Disclosure Statement at www.morningstar.com.au/s/fapds.pdf for more information.

For Recipients in Hong Kong: The Report is distributed by Morningstar Investment Management Asia Limited, which is regulated by the Hong Kong Securities and Futures Commission to provide services to professional investors only. Neither Morningstar Investment Management Asia Limited, nor its representatives, are acting or will be deemed to be acting as an investment advisor to any recipients of this information unless expressly agreed to by Morningstar Investment Management Asia Limited. For enquiries regarding this research, please contact a Morningstar Investment Management Asia Limited Licensed Representative at http://global.morningstar.com/equitydisclosures.

For Recipients in India: This Investment Research is issued by Morningstar Investment Adviser India Private Limited. Morningstar Investment Adviser India Private Limited is registered with SEBI as an Investment Adviser (Registration number INA000001357), as a Portfolio Manager (Registration number INP000006156) and as a Research Entity (Registration Number INH000008686). Morningstar Investment Adviser India Private Limited has not been the subject of any disciplinary action by SEBI or any other legal/ regulatory body. Morningstar Investment Adviser India Private Limited is a wholly owned subsidiary of Morningstar Investment Management LLC. In India, Morningstar Investment Adviser India Private Limited has one associate, Morningstar India Private Limited, which provides data related services, financial data analysis and software development. The Research Analyst has not served as an officer, director or employee of the fund company within the last 12 months, nor has it or its associates engaged in market making activity for the fund company.

*The Conflicts of Interest disclosure above also applies to relatives and associates of Manager Research Analysts in India. The Conflicts of Interest disclosure above also applies to associates of Manager Research Analysts in India. The terms and conditions on which Morningstar Investment Adviser India Private Limited offers Investment Research to clients, varies from client to client, and are detailed in the respective client agreement.

For recipients in Japan: The Report is distributed by Ibbotson Associates Japan, Inc., which is regulated by Financial Services Agency. Neither Ibbotson Associates Japan, Inc., nor its representatives, are acting or will be deemed to be acting as an investment advisor to any recipients of this information.

For recipients in Singapore: For Institutional Investor audiences only. Recipients of this report should contact their financial adviser in Singapore in relation to this report. Morningstar, Inc., and its affiliates, relies on certain exemptions (Financial Advisers Regulations, Section 32B and 32C) to provide its investment research to recipients in Singapore.

About Morningstar® Institutional Equity Research™

Morningstar Institutional Equity Research provides independent, fundamental equity research differentiated by a consistent focus on sustainable competitive advantages, or Economic Moats.

For More Information

+1 312 696-6869
equitysupport@morningstar.com

22 West Washington Street
Chicago, IL 60602 USA