SUSTAINALYTICS

a Morningstar company

THE ESG RISK RATINGS

MATERIAL ESG ISSUE – DATA PRIVACY AND SECURITY

Sustainalytics' Material ESG Issue: Data Privacy and Security

Data privacy and cybersecurity-related issues have become major drivers of business risk in the past several years. In their 2021 Global Risks Report, the World Economic Forum identifies cybersecurity as a "clear and present danger".[1] Sustainalytics considers Privacy and Security a material ESG issue (MEI). The Privacy and Security MEI shows investors which companies are most exposed to this risk and how well they are managing it. In this backgrounder, we will examine why this issue is growing in importance, analyze which industries are most exposed to this issue and highlight companies that perform well on this material ESG issue.

The Growing Importance of Data Privacy and Security

As companies continue to digitize and business models shift to incorporate a complex mix of technology and data supply chains, stakeholders are reckoning with a significant realignment in global risk. Ransomware is driving up insurance premiums, while supply chain and critical infrastructure attacks are placing an increased focus on the cybersecurity ecosystem and the human cost of cyber failure. The cost of cyber insurance continues to grow apace, *far* exceeding global commercial rate increases.[2] As the frequency and severity of losses continue to climb, company's privacy and security risk management practices are coming under increased scrutiny.

The financial impact of a data breach can be significant. According to the 2021 version of the well-known IBM Cost of Data Breach Report, the average total cost of a data breach increased nearly 10% year over year, the largest single year cost increase in the past seven years.[3] The total cost of a data breach was USD 4.24 million with the US being the most expensive jurisdiction, coming in at USD 9.05 million per breach. Globally, the healthcare industry remains the most expensive at USD 9.23 million per breach.[4] Notably, the cost of regulatory compliance failure is key: out of 25 cost factors that either amplify or mitigate data breach cost, compliance failure was the top cost amplifying factor.[5] 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. These privacy issues and associated controversies impact some of the most valuable companies in the market.

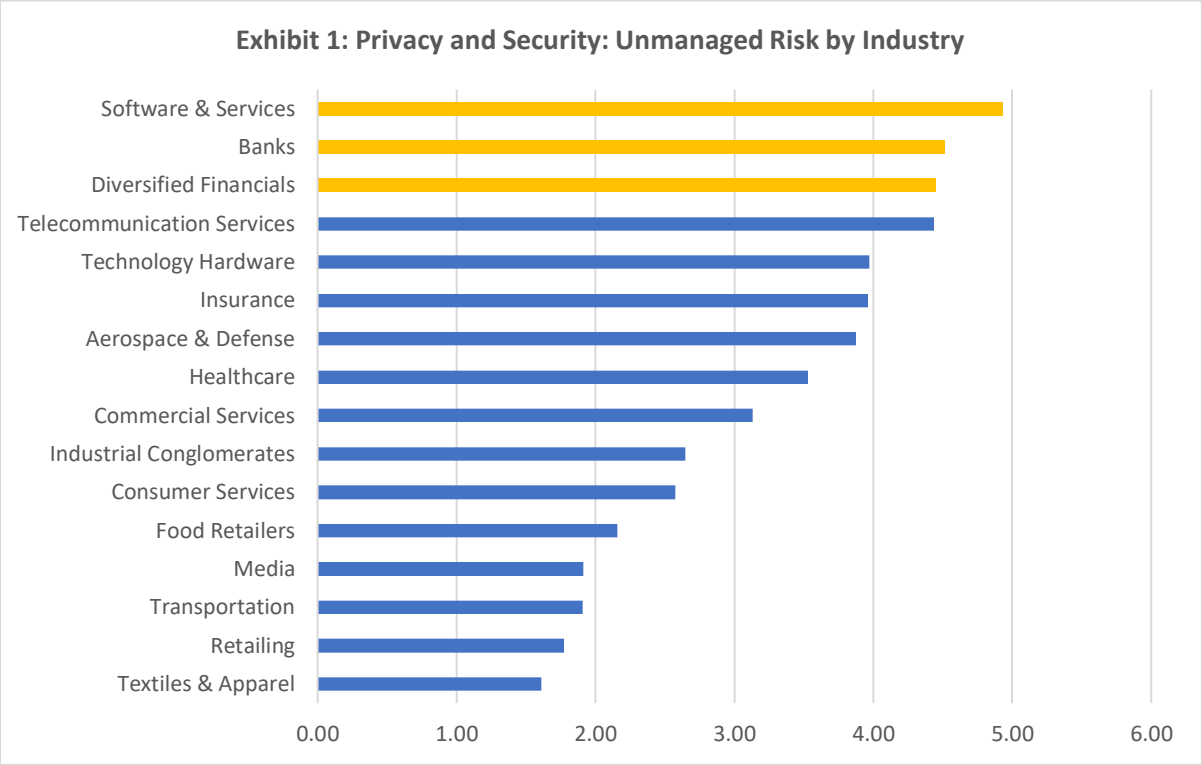
Assessing the Unmanaged Risk of Privacy and Security by Industry

Within the ESG Risk Ratings, Sustainalytics' assessment of Data Privacy and Security considers both the risk a company *cannot* manage due the nature of its business model and the quality of its management practices. These practices include policy commitments, programs, and measures of transparency. Business model-related risk tends to be a function of the volume, breadth, sensitivity, and/or use of the personal information in question, along with any inherent strengths or weaknesses of the systems or software in question. Management practices that mitigate risk include policies related to appropriate collection, use, disclosure, and safeguarding of personal information, along with a commitment to respect a consumer's privacy rights and transparency around the mechanisms they can use to exercise

[1] WEF_The_Global_Risks_Report_2021.pdf (weforum.org)
[2] US Pricing Q3 2021 | Global Insurance Market Index | Marsh
[3] Cost of a Data Breach Report 2021 (ibm.com)
[4] ibid.
[5] ibid.

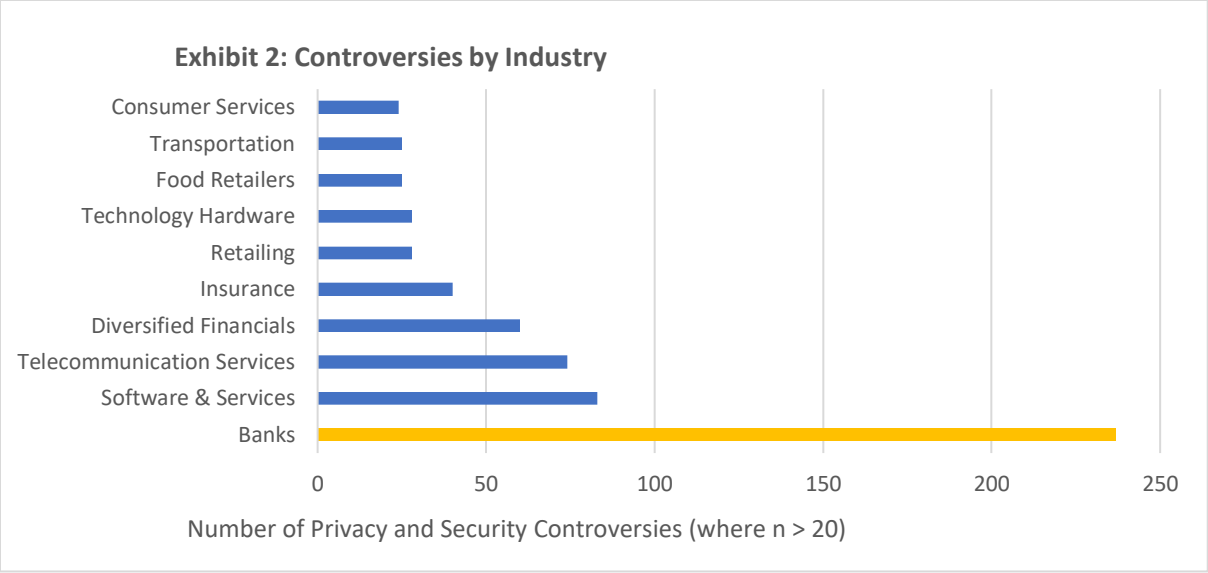
them. These policy commitments should be put into practice through industry-standard privacy and cybersecurity programs and effective reporting.

Applying our ESG Risk Ratings model, we see that Privacy and Security is material for over 2,500 companies in our comprehensive universe of more than 5,000 companies, spanning 21 industries and 60 subindustries. As indicated in Exhibit 1 below, companies in the technology space have the highest unmanaged risk scores on average, followed by financial and insurance services.



(Source: Sustainalytics, Data as of January 26, 2022)

Unmanaged risk also includes incidents and controversies that are related to certain business models (e.g. behavioural advertising), and/or a failure to properly manage risk through policies and programs. These are captured through Sustainalytics screening of more than 60,000 news items, third-party sources, and company and regulator reporting. A total of more than 700 companies in our comprehensive universe are currently dealing with a Privacy and Security controversy, with the heaviest burden in the technology and financial sectors, as indicated in Exhibit 2, below.



(Source: Sustainalytics, Data as of January 26, 2022)

For this issue, controversies include cyberattacks, data breaches, civil litigation, regulatory investigations, public concerns over surveillance, profiling and/or misuse of data, penalties, and fines.

How Sustainalytics' Evaluates Companies on Privacy and Security

Leveraging our ESG Risk Ratings framework, we score companies on a set of subindustry-specific exposure and management indicators. Exposure criteria include the perceived market and "prestige" value of the data, its breadth and volume, sensitivity, business model, and the extent of digitization or data supply chain in the subindustry. Key management controls include policy commitments, programs and measures of transparency. From these criteria, we calibrate the exposure and management indicators for each subindustry.

Focusing on the insurance and healthcare spaces, we identify two companies whose management practices are strong and serve to significantly offset their relatively high degrees of exposure. These companies are MetLife Inc. and Anthem Inc.

Source: Sustainalytics ESG Risk Rating Report, MetLife Inc.

Source: Sustainalytics ESG Risk Rating Report, Anthem Inc.

MetLife is the largest life insurer in the U.S. by assets and provides a variety of insurance and financial services products. The company's exposure to Privacy and Security issues is medium: like most larger insurers, MetLife holds a significant amount of sensitive client data and continues to invest in digitization to improve customer experience. Its network is a lucrative target for organizations seeking to access valuable healthcare information and its business model ensures it is subject to a variety of evolving privacy and data security-related regulations, including HIPAA. Nevertheless, MetLife's strong management of this issue ultimately places it within the Negligible Risk category for Privacy and Security, with a #1 ranking in the Insurance industry as a whole. The company's privacy and security policy commitments, and strong privacy and cybersecurity programs provide a robust mitigant to its relatively high exposure to this material issue.

Anthem is one of the largest managed healthcare providers in the US, providing medical benefits to roughly 43 million medical members. The company offers employer, individual, and government-sponsored coverage plans. In 2015, Anthem was the target of a cyberattack that resulted in a breach of over 80 million records. Since that time, Anthem has invested heavily in its privacy and cybersecurity programs: Anthem's information security and risk are managed by a specialized team subject to the oversight of a chief information security officer. Anthem also requires its employees take part in security-awareness training, covering topics such as cybersecurity and data protection. Finally, Anthem conducts regular security audits and vulnerability assessments of the company's systems, products and practices affecting user data. These leading management practices place it #1 within its subindustry, with a Negligible Risk score for Privacy and Security.

A Cybersecurity Reckoning?

To date, cybersecurity has been associated with concerns about personal information and identity theft. Over the course of the past year, vulnerabilities in corporate cybersecurity are becoming increasingly clear to the public. High profile breaches, including SolarWinds, Colonial Pipeline, and JBS have become front-page news, with visible impact to the companies themselves, along with associated supply-chains and communities. In short, the *public* costs of underinvestment in corporate cybersecurity are increasingly viewed as market failures, much as those in the environmental sphere. These costs are driving increased regulation in this space, along with stronger enforcement. By leveraging our ESG Risk Ratings, investors can clearly see which companies are most exposed to this key issue and how well they are managing their related risks.

SUSTAINALYTICS

a Morningstar company