Our approach to data privacy and security

BlackRock

Investment Stewardship

Our clients depend on BlackRock to help them achieve their investment goals. These clients include public and private pension plans, governments, insurance companies, endowments, universities, charities and ultimately individual investors, among others. Consistent with BlackRock's fiduciary duty as an asset manager, BlackRock Investment Stewardship (BIS)'s purpose is to support companies in which we invest on behalf of our clients in their efforts to create long term durable financial performance.

BIS serves as an important link between our clients and the companies they invest in – and the trust our clients place in us gives us a great responsibility to advocate on their behalf. That is why we are interested in hearing from companies about their strategies for navigating the challenges and capturing the opportunities they face. As we are long-term investors on behalf of our clients, the business and governance decisions that companies make will have a direct impact on our clients' investment outcomes and financial well-being.

BlackRock Investment Stewardship (BIS) believes companies that actively assess and mitigate potential risks that are material to their business operations will be well-positioned to create long-term value for our clients. For many companies, this includes data privacy and security.

Direct engagement with companies is an important mechanism to improve our understanding of the business and its material risks and opportunities. Engagement also provides us with the opportunity to hear directly from the company on its management and oversight of material issues and how their actions are aligned with companies on how they are managing these issues. With advancing technologies creating a rapidly evolving landscape for companies across regions and sectors, BIS is discussing data privacy and security with the companies in which BlackRock is invested on behalf of our clients.

Data privacy and security as a material risk

Technology is playing an important role in both the global economy and society. Most companies today use technology platforms throughout their businesses. With the advancement of digital technology increasing interactions between companies and stakeholders, many companies are collecting extensive amounts of personal, and often sensitive, data which creates responsibilities and risks for those companies. With that has come increased risks associated with data privacy and security. Companies have been increasing their investment in data related security. We expect this trend to continue as companies become even more reliant on the digital exchange of information. The addressable market for network security, cloud security and security operations is expected to increase to $110 billion by calendar year 2024 (+14% compound annual growth rate since calendar year 2021).[1]

From the point of view of a long-term investor, seeking to ensure durable returns for our clients, increased access to personal data by companies comes with material business risks that can impact a company's reputation and their ability to operate. Whereas the global average direct and indirect cost of a single data breach is estimated to be over $4 million in 2021, the financial tail risk associated with a very significant data breach can run to hundreds of millions of dollars.[2] While mega breaches are not the normal experience for most businesses, they can have an outsized impact on consumers and industries. The average cost of a mega breach – those that include 50-65 million compromised records – is estimated at $400 million.[3] A lack of adequate protections could increase that cost even further in the future, should customers become less willing to share sensitive information with or use services and products from an impacted company.

Investors, however, can face significant transparency gaps when assessing companies' management of these risks and preparedness for a crisis event. More recently, we have seen efforts to address that gap, with an increased emphasis on regular reporting and transparency on policies and board oversight, which we welcome given the sensitivity associated with the topic as well as the relatively new nature of these risks and regulation. BIS believes that data security is a material issue for more and more companies and regularly engages boards and management teams regarding the oversight and management of data privacy and security, crisis preparedness and response as well as related company disclosures. We recognize that companies must balance the need to provide investors sufficient information so it is clear that data privacy risks are being managed while also maintaining appropriate levels of confidentiality. This can be done by companies without sharing detailed, proprietary information as to precisely how they are preventing breaches.

Engaging boards and management on data privacy and security

Consistent with our Global Principles, BIS identifies companies for engagement based on our Engagement Priorities, our prior history of voting and engagement with the company, and our assessment of a company's financial and governance profile relative to its peers. While data privacy and security issues can be material to all companies in our portfolios, we focus our engagement on those companies with the greatest potential risk. We consider industry and market-specific context along with sector-specific government policy in assessing these risks. We typically address this issue in the world's leading telecoms, technology, professional services firms, and selectively with other companies with extensive access to customer data.

BIS encourages companies to maintain up-to-date data privacy standard operating procedures, policies, and guidelines that govern the collection, use, disclosure, transfer, storage, and retention of its customers' and employees' personal information. Additionally, BIS encourages companies to maintain robust data security protocols that emphasize information security resilience, compliance, training and awareness, monitoring, and incident response planning across the company's applications, networks, and overall system security.

Our approach in focus

Through our engagements with company management, we aim to understand the following:

Materiality assessment

- What is the company's exposure to data privacy and security risk based on its business model, for example from the quantity, type and sensitivity of the data it collects (i.e., users vs. customers; individual vs. corporate; private vs. public, sensitive vs. non-sensitive)?
- What are the concrete financial implications to the company related to privacy, data, and cyber security?
- Are there any related regulatory actions taken or anticipated? For a company operating/listing in multiple jurisdictions, how does it manage to comply with multiple data security/privacy regulations?

Board oversight and resources

- How effectively does the board maintain comprehensive oversight and understanding of material privacy and data security risks?
- How are these matters factored into the company's business continuity plan?
- What are the resources dedicated to cyber risk management and why are these considered adequate for the business? Are metrics related to employee training shared broadly with stakeholders internally and externally?
- Does the company use an industry security framework and how do they measure themselves against that framework?
- How does the company identify and address technical and organizational security issues to protect against data security breaches?

Customer consent and data processing

- How does the company determine what data is appropriate to collect and balance the use of customers' personal information for revenue opportunities with legal, regulatory, and reputational risks while maintaining customer trust?
- As customers become more aware of the importance and risks associated with their data, how does the company factor in potential shifts in customers' willingness to share their data over the long run?
- How does the company ensure that collected data is used for its stated purpose and that there are no deviations?
- If the company is applying algorithms to users' personal information for targeting purposes, what is the policy to review these algorithms (at both the management level and the board level) to ensure that there is no perceived discrimination based on ethnicity, purchasing power or other demographic categories that might be perceived as sensitive?

Third party management

- In the case of transfer of data to third parties, how does the company ensure that the handling of data is done in a responsible way during the transfer and aligned with the company's protection policies?

BIS encourages those companies that have identified data privacy as a material risk to have robust documentation that outlines their policies and practices regarding data privacy. The company should be able to outline how it protects its customers' and employees' personal information, as well as the company's proprietary information / intellectual property. Documentation may include the company's compliance with local and international regulations, as applicable.[4]

BIS encourages companies to monitor the evolution of regulation and customers' willingness to share personal data (e.g., accepting cookies, etc.) particularly for larger companies. Compliance with regulation on data security goes beyond country of incorporation as it often requires the consideration of the location of users and services provided – creating more complexity. Additionally, while data privacy regulations initially focused on the use and protection of data of individuals, we have noted a stronger focus towards data governance, consumer protection, enhancing competitiveness of markets and online safety in recent years. For example, in the EU, the Digital Service Act is intended to give users more control over what they can see online. Users will see why specific content is recommended and will be able to choose an option that does not include profiling. If finalized, this and other similar regulations, could have significant implications for businesses that operate in covered markets. We are interested in understanding how companies are addressing these risks and whether they see opportunities created by changing regulatory landscapes.

We also engage companies on data privacy where there is evidence that a material event could have an adverse effect on shareholder value. For example, poor risk management with respect to data privacy and security may result in lack of customer confidence, impaired intellectual property value, or market share loss, as well as regulatory action or damage to a company's reputation. BIS encourages companies to have a clear process in place to provide the board regular updates on privacy and data security as well as training to ensure that governance bodies have a comprehensive understanding of those issues. Given the complexity of the topic and the material implications, we encourage boards to have formal oversight of management's approach to data security and privacy, and for respective responsibilities to be clearly defined.

In advance of engagement, we analyze public information regarding the company's exposure to and management of data privacy and security, where available. We also refer to third party research on the company's business practices as well as what are considered industry best practices. If, based on our assessment, a company is not effectively addressing material data privacy and security risks, or its disclosures setting out its approach are inadequate relative to peers and/or industry standards, we will engage with company management and/or board members. We engage to explore the topics outlined above, amongst others, to further understand the company's approach and provide feedback from our perspective as a long-term shareholder on behalf of our clients.

Below are examples of BIS engagements regarding data privacy and security. Given the increased focus on stakeholder interests, discussions with selected companies covered the financial implications of such risks, their policies and practices to manage them, as well as how boards oversee risk.

Data Privacy and Security in Interactive Media & Services

Main challenges for the industry: There are concerns regarding Interactive Media & Services companies' practices with regard to the collection, use, governance, disclosure, or security of personal information or other data-privacy-related matters and how these issues could harm companies' reputation, financial condition, and operating results. Software defects, security breaches, and attacks on their systems could result in the improper disclosure and use of user data and interference with users' and customers' ability to use their products and services, harming business operations and reputation. Systems and control failures, security breaches, failure to comply with companies' privacy policies, and/or inadvertent disclosure of user data could result in government and legal exposure, seriously harm their reputation, brand, and business, and impair their ability to attract and retain users or customers. Cyber-attacks and other attempts to gain unauthorized access to their systems occur on a regular basis; industry-wide vulnerabilities could negatively impact these companies or their partners with whom they share user or other customer information.

Company: Alphabet
Sector: Interactive Media & Services
Region: AMRS
Issue: Oversight of data privacy and cybersecurity
Engagement timeline: May 2022

BIS engaged with Alphabet in advance of their 2022 annual general meeting. We discussed the company's policies and disclosure regarding data collection, privacy, and security. Alphabet regularly includes safety and security reporting via its Transparency Report. Topics within the Security and privacy section include Requests for user information, Google Safe Browsing, Email encryption in transit, HTTPS encryption on the web, Android ecosystem security, and Combating Child Sexual Abuse Material. Their Safety Center website explains how Alphabet protects the privacy and security of users, including details about how they use leading encryption technology like HTTPS and Transport Layer security to keep data safe, proactive security alerts to help protect private information, and the "Safe Browsing" feature to detect and automatically block cybersecurity threats. Alphabet recently conveyed its approach to security, noting that they are looking at the future of cybersecurity and investing in advanced, state-of-the-art capabilities. The company continues to design its products and modify features to enable users to better control their data. The company provides timely updates via their safety & security blog. BIS determined that the company's disclosure is currently robust, and the management adapts Alphabet's disclosure as the environment and their products evolve. At the board level, the Audit and Compliance Committee is regularly updated by management and discusses these issues frequently; therefore, we ascertained that there is adequate board oversight. A vote bulletin detailing our vote rationale at the 2022 annual general meeting with respect to a shareholder proposal requesting a report on how Alphabet is managing risks related to data collection, privacy and security is available on the Investment Stewardship website. BIS will continue to monitor Alphabet's progress in disclosure and product development around data privacy and security given that it is a material risk for the company.

Data Privacy and Security in Professional Services

Main challenges for the industry: Professional services companies, and specifically recruiting agencies, obtain and handle a significant volume of personal identifiable information on job candidates that they are trying to place for specific clients' mandates. The potential mishandling of personal data and unauthorized leakage of such information is an increasingly prominent risk for the sector, which could result in breaches of data protection laws. This trend has been further exacerbated by the continuous digitization of the recruitment process, which has also exposed the industry to increased cyber security risks. As such, to comply with regulatory requirements (e.g., GDPR[5]) and heightened market expectations, recruiting agencies and other professional services companies are required to set out clearly in their privacy policies how they process candidates' personal data and that adequate controls and oversight procedures are in place to ensure this data is handled securely, including data received by third party recruiting platforms.

Company: Hays plc
Sector: Professional Services
Region: EMEA
Issue: Oversight of data privacy and cybersecurity
Engagement timeline: December 2021

BIS engaged with Hays plc management regarding the company's existing processes and procedures to monitor data security issues. As a recruitment service provider, the company has access to large volumes of jobseeker data and thus has high exposure to privacy-related risks. In addition, the company provides temporary and permanent staffing solutions globally and is thus exposed to workforce management challenges related to different client requirements. As such, data privacy and cybersecurity have been on the board agenda for many years. Their information security framework is on par with that of most industry peers, with measures such as penetration testing of data security systems and mandatory staff training on privacy practices. Hays plc security systems are certified to the widely accepted ISO 27001[6] standard. Management has expressed confidence in their information technology team, but the team also leverages the expertise of external third parties to protect against data breaches.

Data Privacy and Security in Consumer Discretionary/Hotels & Lodging

Main challenges for the industry: The lodging industry relies heavily on internal and external technology systems, including those used for reservations, revenue management, property management, human resources, and payroll systems. Companies in this industry may manage global reservation systems or use third-party service providers' reservation systems that allow individuals to book reservations directly online, through mobile apps, telephone call centers, or through intermediaries like travel agents, travel websites, and other distribution channels. These companies may also collect, store, use, and transmit large volumes of data regarding associates, guests, customers, owners, licensees, franchisees, and their own business operations, including credit card numbers, reservation and loyalty data, and other personal information, in various information systems that they maintain and in systems maintained by third parties, including their owners, franchisees, licensees, and service providers.

The information, security, and privacy requirements imposed by governmental regulation, contractual obligations, and the requirements of the payment card industry continue to become increasingly stringent in many jurisdictions in which they operate. Hotels and their owners, franchisees, licensees, and service providers will need to keep their systems up to date to satisfy these changing legal and regulatory requirements, as well as associate and guest expectations, which may require significant additional investments or time to do so.

Company: Marriott International, Inc.
Sector: Consumer Discretionary
Region: AMRS
Issue: Remediation of data incidents; enhanced oversight of information security
Engagement timeline: November 2020; December 2021; April 2022
BIS engaged with Marriott following several data security incidents, including a data incident impacting over 300 million guest records discovered in November 2018 and another breach involving approximately 5.2 million guests in March 2020.

Since then, Marriott has implemented enhanced security measures to better safeguard their systems and data, and they intend to continue implementing additional measures consistent with best practices in the future. In 2021, the Board established the Technology and Information Security Oversight Committee to specifically oversee Marriott's information security, privacy, and technology-related risks. This Committee assists the Board in overseeing management efforts to monitor, manage, and mitigate those risks. BIS believes Marriott's enhanced board oversight and improved security measures were a significant step in the right direction for the company. As Marriott has experienced data security incidents in the past, additional incidents, or the failure to detect and appropriately respond to additional incidents, could magnify the severity of the adverse effects on their business. BIS will continue to monitor how Marriott manages technology, information protection, and privacy risks going forward.

Data Privacy and Security in the Telecommunication Industry

Main challenges for the industry: The telecom industry manages a significant amount of data related to their customers – such as location, web browsing history, and demographic data, for example. Telecom companies are facing increasing scrutiny by both customers and regulatory scrutiny related to how the data is handled and transferred to third parties. Additionally, this industry has been targeted by a high number of external threats seeking to gather personal data, including discussions, videos, and personal information on individuals.

Company: Vodafone Group PLC
Sector: Telecommunications
Region: EMEA
Issue: Remediation of data incidents from third parties' data processing, resulting in unlawfully contacting customers for telemarketing purposes
Engagement timeline: March 2022
Privacy and data security are among the most material risks affecting companies in the telecom industry. BIS engaged with Vodafone after the company received several penalties through its subsidiaries in Italy and Spain because of unlawfully processing personal data for telemarketing purposes without the required consent.

During our engagement with the company, BIS sought to better understand the steps they have taken to strengthen their oversight and data management practices both within the company and in relation to third parties that manage their customer data. We were encouraged by the company's remediation efforts and found their explanations on how they manage data privacy risks to be reasonable. For example, the company applies GDPR rules – considered the most sophisticated globally - in all jurisdictions, even those that are not covered by GDPR, to ensure the same protections are held in every jurisdiction that the company operates within. The company has also put in place additional processes to avoid unsolicited outgoing calls to its customers, such as re-routing agency calls from Vodafone's internal system, and only paying third parties on authorized calls. Finally, Vodafone ensures that external suppliers and third-party users manage data according to their policy through enhanced due diligence processes and auditing. The company has responded to its issues in a comprehensive manner, and we look forward to continued dialogue in the future.

Authors and Contributors

John McKinley
Managing Director
BlackRock Investment Stewardship

Tanya Levy-Odom
Director
BlackRock Investment Stewardship

Gaia Mazzucchelli
Vice President
BlackRock Investment Stewardship

Giovanni Barbi
Vice President
BlackRock Investment Stewardship

Eddy Gan
Vice President
BlackRock Investment Stewardship

Endnotes

1. Palo Alto Networks Analyst Day presentation September 2021
2. "Cost of Data Breach Report 2021", IBM Security and Ponemon Institute
3. See previous footnote.
4. i.e., General Data Protection Regulation (GDPR), California Consumer Privacy Act of 2018 (CCPA) and Payment Card Industry Data Security Standard (PCI DSS)
5. The General Data Protection Regulation (GDPR) is a European law that was implemented May 25, 2018. It requires organizations to safeguard personal data and uphold the privacy rights of anyone in EU territory. It includes seven principles of data protection that must be implemented and eight privacy rights that must be facilitated.
6. The ISO/IEC 27001:2013 specifies the requirements for "establishing, implementing, maintaining and continually improving an information security management system within the context of the organization."

Want to know more?

blackrock.com/stewardship | contactstewardship@blackrock.com

BlackRock.