ROCKEFELLER
ASSET MANAGEMENT

November 2021

Constructive Engagement Series

Engagement Campaign to Protect Privacy and Secure Sensitive Data

In our increasingly digitalized world, data is one of every organization's most valuable assets. As the amount of data collected increases, so has the frequency[i], severity, and costs[ii] of cyberattacks across sectors. Recent events have triggered many firms to re-assess and bolster data privacy and cyber security policies, and similarly, our attention has turned to the financial materiality of data protection across our holdings. Research shows that companies with top quartile cybersecurity risk management practices outperform their respective index by 1-2% annually.

We engaged with numerous companies across our equity strategies about their privacy and data security policies, practices, and disclosures to encourage continuous improvement and protect against financial losses, operational disruption, reputational risk, intellectual property theft, loss of sensitive data, and fraud.

National Institute of Standards and Technology (NIST) Cybersecurity Framework

Material Risks with Limited Disclosure

Privacy and cybersecurity incidents lead to material financial impacts and have increasingly worried regulators and challenged companies across sectors. In 2021, several high-profile breaches at companies including T-Mobile and Microsoft exposed nearly 40 million records in each incident. Target's 2013 data breach of over 70 million records resulted in just over $200 million in direct remediation costs. While it is difficult to quantify the exact financial impact, revenues decreased 1% and net income declined 34% from 2012 – 2013. The meaningful decrease in net income was largely attributed to additional costs associated with investigating and remediating the breach.[iii] Investigation of the attack revealed several areas where increased measures to protect and remedy outdated services could have prevented the initial system access or the escalation throughout the network.

The global policy landscape is also changing rapidly. The SEC requires disclosures on material cyber risks and incidents, and is considering stronger rules. Yet, disclosure standards differ widely between sectors, typically include boilerplate risk language, and there are no requirements for disclosure on the approach, performance, and practices used for mitigating cyber risks. Around the world, regulators are strengthening privacy policy implementation through China's PIPL, the EU's GDPR, and US states adopting laws aligned with California's CCPA.

OUR PHILOSOPHY ON ESG ENGAGEMENT

At Rockefeller Asset Management, we believe that rigorous, ESG-integrated analysis coupled with deep shareholder engagement can deliver strong long-term results for our clients. Our research indicates that companies improving their ESG performance will see stronger financial returns over the long-term. Shareholder engagement is a core part of our investment process, evaluated before purchasing a stock and employed throughout the holding period for certain strategies. We appreciate companies that recognize that achieving ESG leadership requires continuous improvement.

---

[i] Verizon, "2021 Data Breach Investigations Report", 2021

[ii] IBM, "Cost of a Data Breach Report 2020", 2021

[iii] Plachkinova, M., Maurer, C., Security Breach at Target, Journal of Information Systems Education, Vol. 29 (1), Winter 2018

ROCKEFELLER
ASSET MANAGEMENT

Engaging with Companies to Enhance Performance

Our **"Engagement to Protect Privacy and Secure Sensitive Data"** campaign targeted companies where privacy and data security were identified as material ESG issues and where our research identified gaps in performance or disclosure compared to best practice. In a letter to the CEO, we asked companies to describe the actions planned, or taken, to address the gaps we identified and feedback on their plans to improve on the two broad categories of privacy and data security performance indicators summarized below:

Governance and Policy	Performance and Implementation
1. **Oversight**: At the board or executive level. 2. **Scope of Policy**: Covers all relevant business lines 3. **Disclosures**: Covering both risks and mitigation. 4. **Operational Plans**: Cover both proactive and reactive measures to limit privacy and cyber risk.	1. **External Audit:** Of policies, practices, and technologies at least every two years. 2. **Standards and Certifications** 3. **Measures and Practices:** Employed to protect sensitive data and respond to incidents. 4. **Training**: Covers all employees, including contractors.

The top gaps that we identified across all sectors with the largest potential impact were the following:

Most Frequency Gaps Identified	Analysis
1. **Independent external audit of privacy and data security policies, practices, and technologies**	75% of our targeted companies did not meet the best-in-class practice for disclosure of independent external audits. Limited public disclosure masked performance where after our inquiry, we found 39% did not perform external audits.
2. **Privacy and data security training completed by all employees, including contractors**	64% of our targeted companies did not meet best-in-class practices for disclosing the scope, frequency, completion rates and types of training completed.
3. **Both proactive and reactive measures and operational plans addressing privacy and data security**	60% of our targeted companies did not meet best practice to disclose formal proactive and reactive operational plans to both prevent and respond to cyber threats.

Encouraging Results Hidden by Limited Disclosure

Companies' responses to the campaign illustrated the increasing importance of privacy and data security amid the evolving cyber risk landscape. Over 75% of the companies we engaged replied, and many were interested in further discussing our questions and their performance. We were surprised that several companies indicated our inquiry was the first time an investor had requested information on cyber risk management and disclosure. One of the key areas of concern was balancing transparency and protecting valuable cyber assets and intellectual property.

Several Chief Information Security Officers (CISOs) highlighted their understandable reluctance to provide information that could allow bad actors to penetrate defenses. Yet after extensive dialogue with companies across sectors, we found that strong disclosure of items like cyber governance and data privacy policies was an indicator of management quality. While we did not advocate providing detailed technical information on defensive measures, the disclosure of robust cyber oversight, policy, and practices may have the positive effect of deterring potential cyber attackers while reassuring investors of a firm's focus and performance on cyber defense. As a result of our engagement dialogues, severalcompanies updated disclosures, or have indicated that they plan to improve their practices or disclosures in the future to ensure stakeholders understand their cyber posture.

ROCKEFELLER
ASSET MANAGEMENT

Continuous Improvement Drives Future Plans

Across all our conversations, we stressed the need for continuous improvement on cyber risk management and meaningful indicators to assess risk and performance. Nearly a third of the companies we engaged acknowledged their potential to improve disclosures with several making updates immediately. Many more told us they planned to improve disclosures in their next reporting cycle as well as invest in new capabilities including third party support. Below are examples of improvements that resulted from the campaign:

Disclosure Improvements	Improvements Planned
First Horizon Corp. is regional financial services company operating in 12 states across the Southern US. After discussions with First Horizon on data protection and privacy, the company released an ESG report to illustrate their cyber risk oversight structure and training program showing alignment with best practices.	**A UK-based financial services company** is currently driving collaborative action in the UK market on privacy and cybersecurity. To further strengthen their privacy and cybersecurity programs, they are considering improving third-party audit practices and implementing additional third-party certifications.
A US-based insurance holding company offering life and health insurance, annuity, and investment products had good performance but focused on disclosing cyber risks. After our dialogue on cyber risk management, the company updated their ESG report to illustrate their strong cyber maturity and proactive posture.	**A US-based software company** that provides solutions to protect data from insider threats and cyberattacks plans to update their enterprise-wide cybersecurity policy, including several of the items that were raised during our conversations. To show stakeholders their expertise and focus on data protection, they plan to make additional public disclosures, including posting the updated policies.

Next Steps

Managing and protecting data is an enterprise-wide responsibility which increasingly requires strong oversight, continuous improvement, and industry collaboration. We were encouraged by the broad efforts being made by companies across sectors to improve their privacy and data security practices and disclosures and plan to continue our dialogues with management teams on topics such as meaningful performance indicators, external audits, training, and operational planning.

"Our conversations with Rockefeller were very informative to understand how investors are assessing performance on privacy and cybersecurity. As a result, we updated and publicly posted additional information on our cyber risk management practices by adding many of the points we discussed. As a financial services company, protecting our customers' data has always been a part of our DNA. Now, we want to show the public how the same strong risk mitigation solutions we offer to our customers are used to protect our own data."

***Mary Lakey** –ESG Officer, First Horizon*

SUSTAINABLE DEVELOPMENT GOALS

Engagement Target: Ensure companies have strong privacy and data security oversight, policies and practices that are properly disclosed as merited by market conditions for protecting cyber assets.

Goal 16

Peace, Justice & Strong Institutions

Goal listed above represent the United Nations Sustainable Developments Goals, which seek to promote prosperity while protecting the planet, established in 2015.

Mia Overall
Director of Shareholder Engagement

Christopher Huynh
ESG Engagement Analyst

ROCKEFELLER
ASSET MANAGEMENT

Annex 1: Engagement to Protect Privacy and Secure Sensitive Data Letter

Dear CEO,

At Rockefeller Asset Management, engagement on material ESG issues is a critical part of our investment approach. Through proactive engagement with our investees, we strive to encourage improved ESG performance which we believe enhances shareholder value while catalyzing positive change. In this instance, we are focusing on customer privacy and data security, which we believe is material to your company, amongst other ESG issues. Privacy and data security are two complex issues which, as you know, have increasingly worried investors, and challenged companies across industries as the frequency, severity, and costs of cyberattacks has risen with impacts to valuations. As investors, we wrestle with the challenge of requesting disclosures that will give us comfort with cybersecurity practices while not creating additional risks or vulnerabilities for the companies we hold. To do this, we rely mainly on your disclosures of general policies and practices as well as third-party data, which we know will not cover the full scope of your efforts and may have inaccuracies. Nevertheless, we have reviewed the customer privacy, data security and disclosure practices of our investees against best practice for policies and disclosures and would like to bring several matters to your attention to better understand your practices.

You are receiving this letter because our analysis of public disclosures and third-party reports reveals gaps in your company's privacy and data security policies, processes or disclosures compared to best practice to protect against operational disruption, reputational risk, intellectual property theft, loss of sensitive data, and fraud. The top issues we noted appear to be misaligned with the following best practices:

1. **Independent external audit** of policies, processes, and performance, at least every two years.
2. The scope of **privacy and data security training** covers all employees, including contractors.
3. **Both proactive and reactive data breach measures and operational plans** are in place to address topics that include Incident Response, Data Breach, Business Continuity, and Disaster Recovery.

We know you care deeply about protecting your company's data and that of your customers. For this reason, we invite you to review your privacy and data security strategies, policies, and processes and where appropriate and relevant to your company, take action to strengthen them to align with the best practices listed on the following page. **Additionally, we ask you to respond to us describing actions planned, or taken, to address the issues above, or to improve the alignment, cybersecurity maturity and posture, and disclosures related to any of the best practices described in the Annex below.**

Managing and protecting data is an enterprise-wide responsibility which increasingly requires strong oversight, continuous improvement, and collaboration. We are pleased to be long term investors in your company and, with this letter, aim to support your efforts on this topic. Thank you in advance for your attention. We look forward to your response.

Sincerely,

Mia Overall

Christopher Huynh

ROCKEFELLER
ASSET MANAGEMENT

Annex 2: Data Privacy and Cybersecurity Best Practices

Below is a list of best practices categorized in two broad categories: Governance and Policy, and Implementation and Performance. These best practices are largely aligned with third party ESG data providers' evaluation of data privacy and cybersecurity, such as MSCI and Bloomberg. We strongly encourage you to review these items against your own policies and practices to identify any gaps that may reduce risks or improve your competitive positioning

Governance and Policy

1. **Oversight:** While subject matter expertise is critical to execution, **oversight at the board or executive level**, is essential to empower teams to improve beyond their individual or departmental areas of focus.

2. **Policy and Disclosure: Public disclosure of policies, practices, and privacy and data security performance** develops trust with stakeholders and provides a public commitment which stakeholders value highly to evaluate overall cyber-risk and enterprise risk management. Policies should be easy to find through public sources. They should be easy to understand, describe practices, and provide users with the information needed to make decisions. Important aspects of policy include:
   a. **Policy Scope:** The scope of policy is a key determining factor in its impact. Policies covering all relevant geographies, business lines, suppliers, and business partners reduce risks from potential actors, including those outside of an organization's direct control.
   b. **Alignment with Regulation:** Regular, proactive updates to policies, practices, and disclosures to align with, and where possible, stay ahead of current and evolving regulation is critical amid the rapidly evolving policy landscape.
   c. **Privacy Policy:** Given the wide variance across sectors of privacy policies that govern and provide rights to individuals to control their data and personal identifiable information (PII), the scope of policies should include the most important aspects of data rights including **collection, access control, rectification, deletion, retention, notifications, grievance and remedy, algorithm use, data use, and sharing with third parties.**
   d. **Data Security Policy:** Comprehensive data security policies that support the protection of data across the entire enterprise encompass the interdependencies between business lines and departments. **Policies should consider web application security, network security, information security, endpoint security, access control, records retention, notification, and sharing with third parties.**

3. **Cybersecurity Insurance: Insurance protection is one of the newest best practices to protect against the operational and financial risks from cyber-attacks.** Evaluating cybersecurity insurance coverage, subject to availability, helps to align with industry specific insurance policy requirements and standards. The process may be a useful indicator to evaluate an organization's strength of data security technology and processes as well as cyber risks as it relates to overall enterprise risk management.

4. **Risk Management Plans: Incident Response, Data Breach, Business Continuity, and Disaster Recovery plans** can keep an incident from turning into a catastrophe. Crisis management plans and mock-scenario analysis can be used to evaluate the responsiveness of technology, processes, and teams. Regularly evaluating the scope, proactiveness, reactiveness, and strength of risk management plans helps to ensure they are aligned to the latest standards in a constantly changing cyber risk environment.

ROCKEFELLER
ASSET MANAGEMENT

Performance and Implementation

1. **Certification and Standards: Certification to the latest iterations of widely recognized industry standards is a key indicator to evaluate implementation practices.** Disclosing the general, and industry-specific, privacy and cybersecurity certifications and standards used by an organization allows stakeholders to evaluate an organization's cyber-maturity, risk exposure and risk management profile. The ISO/IEC 27000 family of standards provides requirements for information security management systems applicable to assets such as financial data, PII, employee data, intellectual property, and information provided to third parties.

2. **Data Security Measures:** Utilization of the newest, and best, industry-applicable data protection technology and processes are indicators of strong cyber-risk management. **Continuously investing, evaluating, and implementing, the best-available security measures is critical.** Measures to consider include web application security, network security, information security, endpoint security, access control, end-to-end encryption, adaptive multi-factor authentication, mobile device security, identity management, Privacy-by-Design, access controls, patching cadences, and Zero-Trust architectures, amongst others.

3. **Training:** Even the best processes and tools can be defeated if training is ineffective. One of the most meaningful influences on effectiveness in data protection is widening **the scope of employees that are trained to include not only all permanent employees, but also temporary employees, contractors, and sub-contractors.** Training content relevant to all potential threats to privacy and data security may include: the classifications and types of data encountered by users, the protection of sensitive data, access control, and processes and controls, amongst other topics.

4. **Auditing:** Auditing a firm's technology, policies, and processes is one of the most important tactics to assess and determine strategies for improving privacy and data security performance. **Both internal and independent external third-party audits are recommended.** The frequency of audits shows commitment to continuous improvement and is recommended at least every two years. **The scope of auditing should consider policies, technologies, processes, compliance, controls, and performance as well as the examination and analysis of all relevant penetration possibilities and vulnerabilities.** Auditing standards are an indicator to validate audit performance. Standardized auditing frameworks such the Statement on Standards Attestation Engagement (SSAE-18) SOC 2 reports are useful tools to evaluate an organization's controls, security, availability, processing integrity, confidentiality, and privacy. We encourage disclosing the standards used by your firm to align with best practices on transparency.

rockco.com