Digital technology

Data privacy | Cyber crime | Responsible AI

Thematic overview

Technology is part of our everyday lives. Cloud connected solutions have helped businesses improve cyber security, manage large amounts of data, and optimise business processes. E-commerce and online platforms have helped extend a company's reach and customer base. And now, artificial intelligence (AI) is predicted to transform entire industries and offer substantial efficiency gains.

Technology is often a double-edged sword. As much as cloud services can help to manage big data, having all the data in one place also increases risks related to data privacy and cyber crime. It is therefore important that we consider these risks and opportunities when assessing the ESG and sustainability implications for various companies.

We introduced digital technology as a priority thematic in 2023 and initiated a research project with Australia's premier scientific government research organisation, the CSIRO, to develop a Responsible AI Framework for investors. This project was completed in 2024 and the learnings have now been integrated into our overall ESG Framework.

This section presents examples of engagement related to responsible AI. A full case study on the project is presented on page 22.

We recognise that digital technology is not typically separated as a unique thematic within ESG and sustainability structures, however, we feel that the issues are specific enough to warrant a targeted approach.

2024 update

Materiality

In 2024, **cyber crime** was ranked one of the most material topics across the ESG issues assessed against our holdings. It is an issue which is relevant to almost all companies and the risk management approach is difficult to assess. Under this issue we assess the risk of events such as scams, ransomware attacks, bad actor breaches and theft, and general data breaches from technology or process failure.

This year we noted an increase in the amount of news flow related to cyber crime. This was also reflected in an increase in company commentary on the issue.

The CrowdStrike outage in July 2024, which caused 8.5 million global computer systems to crash, was not linked to a cyber crime event however, it did shine a light on the world's growing reliance on cloud connected and digital systems.

Similarly, **data privacy** has also continued to increase in materiality, largely due to the AI investment thematic and increasing storage and use of big data. We have not noted a change to the number or impact from material data breaches in 2024, however, the ongoing regulator and customer focus means that this issue is receiving increased attention.

Responsible AI is still an emerging issue for most companies. However, in 2024 we saw a material increase in the general awareness and interest in responsible AI as well as a slight increase the level of disclosure. For example, Microsoft published a Responsible AI Transparency Report early in the year.

There has also been significant interest from other investors, including asset owners and managers, in our project with the CSIRO. In 2024 we participated in more than **30 meetings and presentations** to share insights and learnings from our project. We were also invited to present at the **UNPRI Annual Conference** in Toronto.

Research

- Engagement with cyber experts to identify best practice management measures to mitigate the risk of cyber incidents. We have applied these guiding principles in our ESG risk assessments and company engagements in 2024.
- Joined the RIAA Digital Technology and Human Rights Working Group in 2023. In 2024 this group published a report highlighting the human rights implications of AI and how investors can better engage on the topic.
- Finalised a research project with the CSIRO to develop a Responsible AI Framework for investors. We published a research report and toolkit to support the implementation of the framework. We have continued to engage with companies on their approach to AI throughout 2024.
- Initiated a project to expand our Responsible AI Framework to also cover the AI value chain (e.g. emissions and water use through semiconductor manufacturing). We intend to complete this work in 2025.
- Attended a day of presentations at CSL headquarters in Melbourne to understand the AI opportunity in drug development and discovery.

Examples of company engagement

DATA PRIVACY

Intuitive Surgical manufactures the Da Vinci and Ion Robotic Systems used in surgeries worldwide. The company has been assigned an **ESG risk level 2** under our ESG Framework mainly because of risks related to product quality, safety and the potential for reputational impacts. We generally engage at least once per year on this topic to track potential issues and controls. In 2024 we also added data privacy and responsible AI to the meeting agenda. As an outcome, we initiated an **engagement objective** related to responsible AI and shared our Responsible AI Framework. We will continue to prioritise this engagement.

CYBER CRIME

Our Head of ESG and Sustainability was invited to a small group **Boardroom ESG lunch** with three NAB Board Directors including the Chair. The purpose of the meeting was for the Board to better understand the perspectives of its shareholders and collect feedback related to ESG topics such as climate, customer, trust, policy, and nature. From this engagement we identified three areas for further work including scams management. We have identified a new **engagement objective** for Australian banks as a result. See the case study on the next page.

DATA PRIVACY

Thermo Fisher is a global company offering a range of healthcare equipment, pharmaceutical production, and consulting services. We **engaged** with the sustainability team to assess cybersecurity and data privacy risks. The meeting confirmed the presence of sensitive data within the clinical trial business, prompting further discussion of the company's cybersecurity management plan. We maintained an **ESG risk level** of 2, which also reflects other product quality and regulatory risks. Thermo Fisher has a strong track record and is an example of a company that may shift towards an **ESG risk level** of 1 over time.

RESPONSIBLE AI

In 2023 we initiated an engagement with Wesfarmers related to Responsible AI. Through the CSIRO AI research partnership we **engaged** with the GM OneDigital, Privacy and Trust to understand Wesfarmers' application of AI and how ethical and ESG considerations were being addressed. We established an **engagement objective** to encourage Wesfarmers to publish a Responsible AI framework or policy and confirm governance controls for high-risk AI use cases like facial recognition. We engaged with Wesfarmers a number of times throughout 2024 and discussed AI and technology in most meetings. We conducted a specific update on responsible AI, meeting with the GM OneDigital Privacy and Trust again, and confirmed the business has expanded its active use cases and is implementing a Responsible AI Framework. This remains a high priority engagement with Wesfarmers due to the ongoing reputational and legal risks.

CASE STUDY

Commonwealth Bank of Australia (CBA), National Australia Bank (NAB) and Westpac engagement example: Scams management

Australia's four big banks are the leaders of the Australian financial sector. Between them they hold about 70% market share and 73% of household deposits and owner-occupied home loans. They are a fixture of the Australian corporate landscape and are strictly regulated by bodies such as the Australian Securities and Investments Commission (ASIC) and the Australian Prudential Regulation Authority (APRA). Given the banks' dominance and strong brand recognition, social licence and managing the relationships with customers are essential to maintaining its operating outcomes.

Over the past few years there has been a growing focus within Australia on the role that the banks play in managing financial scams and financial crime more generally. Throughout 2024, there were a series of negative media stories which highlighted victims of financial crimes and pointed the finger at the banks in failing their customers.

In response, we **completed a review** of CBA's, NAB's and Westpac's disclosure on scams management and identified the need for further engagement. Although we felt that the banks were acting responsibly in notifying customers related to scams, and proactively seeking to stop scams clarity on the overall approach, governance, and decision making was missing.

As described above, we engaged with NAB Directors as part of a small group ESG boardroom lunch session. In that meeting we asked the Board what the organisational strategy was in relation to scams? What are the pillars of the bank's scams strategy? Who decides when losses are pays to customers? Is there a policy position on payments? What proportion of losses from financial scams are paid by the bank? And what reporting is provided to the Board?

We asked similar questions in meetings with CBA and Westpac throughout the year and felt that shareholders would benefit from more information on scams management.

As a result of these engagements we have established an **engagement objective** for each bank to confirm and publish further details of its overall approach to scams management including goals or objectives and metrics and measures.

CASE STUDY

Life360 sustainability example: Integrating big data and privacy risk within our SDG analysis

Life360 is a family social networking app with more than 60 million monthly active users. Security-conscious families use the Life360 app to track each other's whereabouts and to track the location of their pets and personal belongings. Life360 also offers a suite of additional security features, such as driver safety monitoring, roadside assistance, and emergency response dispatching.

Life360's goal is to help families and friends stay connected and improve safety, but this also means that it collects and stores lots of sensitive data such as children's location information. It also means that people could use the app and hardware to illegally track partners. To maintain its trust with its customers it is therefore important that Life360 applies a high degree of ethics over its data privacy practices and controls its cyber-crime risks. It is also important that it provides features that allow people to control their own privacy and manage how and when others can track their locations.

Before investing in Life360 in our Australian Sustainable Share Fund we initiated an **ESG and sustainability review** to confirm the material ESG risks and considerations, the ESG risk level, and the SDG alignment outcome and score to determine the suitability for our Australian Sustainable Share Fund.

This review identified two positive and two negative alignments with the SDGs.

- **Positive:** SDG3.6 for the road safety and crash detection benefits of the app and SDG16.1 for protecting people against violence and criminal activity
- **Negative:** SDG5.2 for the risk of coercive control and illegal monitoring with the app and SDG16.4 for risk related to misuse of sensitive data (child location data) and criminal activity

To confirm the risk related to the negative alignments, we **engaged** with the company and reviewed relevant disclosures. We confirmed that the company had a suitable approach to data privacy and risk management and has also built in features into the app to mitigate coercive control risks.

A requirement of the Australian Sustainable Share Fund is that the company must have a net positive alignment to the UN Sustainable Development Goals. The outcome of the assessment for Life360 was a net positive **SDG score** of 70. This reflects the conclusion that the positive widespread benefit to family and child safety well outweighs the less likely occurrence of coercive control, illegal monitoring, and criminal activity from data breaches.

This company was approved by the Sustainable Compliance Committee and subsequently added to the Australian Sustainable Share Fund. This review also set a precedent for our analysis for companies like Life360 which create unique risks around data privacy and safety.

CASE STUDY

Responsible AI Framework engagement example: Sharing our framework with companies to encourage better reporting

In May 2024 we finalised a **collaborative partnership** with the CSIRO to develop a Responsible AI Framework for investors. This framework consists of three steps and is intended to be used by investors to assess the risks and opportunities from the development and application of AI. It is also intended to be used by companies as a guide for the types of disclosures and information investors need to understand and assess their approach to responsible AI.

Since finalising the project we have continued to **engage** with companies and have shared our framework to encourage better reporting and help companies to understand what information investors need to properly assess the risks and opportunities linked to AI.

In 2024, we shared our framework with companies such as Medibank, Netflix, Intuitive Surgical, MercadoLibre, AGL, Origin, Wesfarmers, and Thermo Fisher.

Netflix

Prior to investing in Netflix, we conducted an **ESG review** and identified the misuse of generative AI in content production as a potential risk. This was particularly relevant given the business disruption caused by labour strikes in 2023 involving major Hollywood unions, which were partly driven by concerns over AI's impact on job security.

These issues were resolved in 2023, leading to increased compensation, employee benefits, and restrictions on AI use within three labour organisations. However, at the time, it did cause significant disruption to Netflix' business performance and caused delays in production.

We **engaged** with the company twice to better understand the outcomes of the resolution, the company's view on a similar event occurring in the near term, and how it is approaching AI use given some of the restrictions imposed by the union agreements. Netflix confirmed that it has internal guidelines with cross-functional management on the use of generative AI to guide appropriate AI use cases in the business.

While Netflix noted that it is satisfied with the outcomes of the union agreements, we did provide **feedback** that publishing these AI guidelines externally would be a positive. A longer-term opportunity exists around content quality and production efficiencies from generative AI. We continue to engage with the business on its stated policy commitments and guardrails around AI use to ensure the business builds transparency and trust, whilst using AI in a productive and opportunity-driven manner.