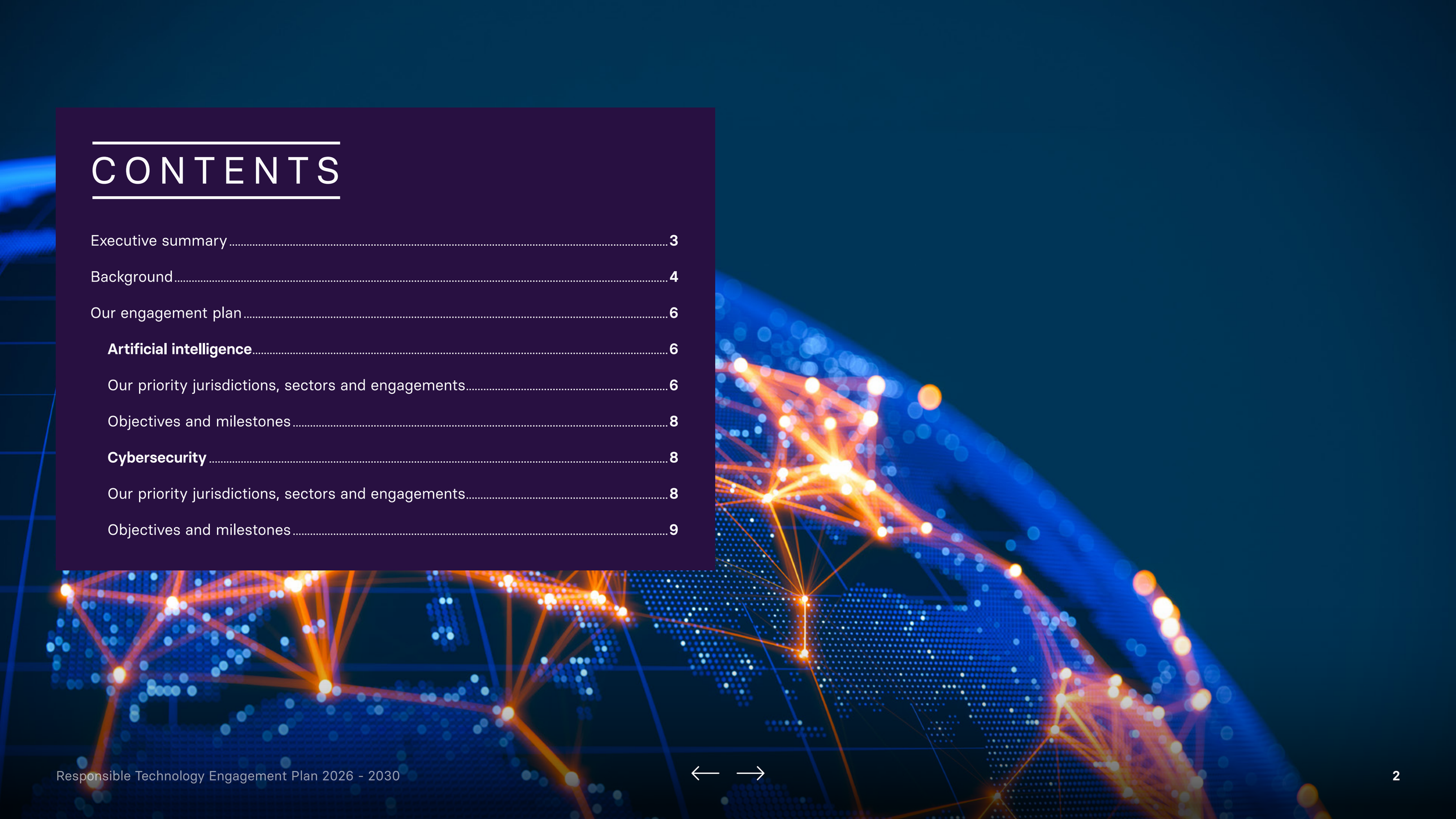
RESPONSIBLE TECHNOLOGY ENGAGEMENT PLAN

Railpen's system-wide stewardship plan for **2026 – 2030**

RAILPEN

CONTENTS



EXECUTIVE SUMMARY

Our goal is to support the responsible adoption of technology – balancing innovation with robust oversight and governance to deliver long-term value and support wider economic growth.

Within the broad technology landscape, we will focus on the following:

- **Cybersecurity**
- **Artificial Intelligence**

Why IT matters

IT underpins almost every sector and business, driving efficiencies and enabling rapid transformation. Adoption of emerging IT is accelerating fast – **78% of organisations used AI in 2024**, up from 55% the year before. Its systemic importance is reinforced by the following:

- Rising concentration of digital risk among few providers
- Workforce transformation through automation
- Mounting pressure on energy infrastructure
- Shifting trust in digital systems

What is systemic risk?

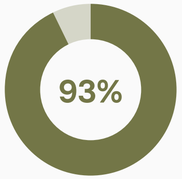
The possibility that a single event or development may trigger widespread failures and negative impacts spanning multiple organisations, sectors, and/or nations.

Source: WEF, 2022

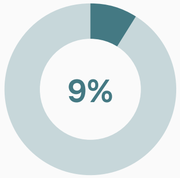
What our research shows

AI enables the intelligence and adaptability of modern IT ecosystems, while cybersecurity underpins their stability and security.

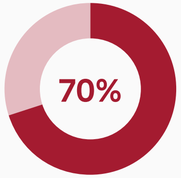
Our work with Royal London Asset Management (RLAM) on 'Cybersecurity Risk and Resilience' and with Chronos Sustainability on 'Achieving Effective AI Governance' highlights the scale of the emerging risks:



93% of companies anticipate significant threats from generative AI (GenAI).



Only **9%** feel prepared to manage them[1].



70% of Chief Information Security Officers (CISOs) anticipate a material cyberattack within a year[2].

These findings reveal a clear gap between awareness and preparedness.

1 Riskonnect (2023), The New Generation of Risk Report.

2 Proofpoint (2024), 2024 Voice of the CISO.

Our approach

Over the next few years, we will shift from reactive to proactive stewardship by taking the following steps:

- Strengthening how companies **understand, manage and disclose** AI and cybersecurity risks
- Prioritising companies at the intersection of **high risk** and **systemic importance**
- Expanding **policy advocacy** as a key lever for systemic change

Our engagement focus

- **Cybersecurity:** collaborative engagement via the Cybersecurity Coalition and advocacy for harmonised disclosure and practices that strengthen system-wide resilience.
- **AI:** company-level engagement aligned with our AI Governance Framework, alongside UK-focused policy work to help shape proportionate, innovation-aligned regulation.

Supported by clear objectives and accountable measures, our plan aims to reduce systemic vulnerabilities, while supporting companies to harness technological opportunities responsibly and protect long-term value for members.

BACKGROUND

Technology spans many areas (figure 1), but our focus is on information technology (IT), which forms the foundation of modern digital infrastructure. IT includes the use of computers, software, and networks to store, retrieve, transmit, and process data – capabilities that enable organisations to operate efficiently[3]. Today, several key themes shape the IT landscape, include artificial intelligence (AI), cybersecurity, quantum computing, cloud and edge computing, and advanced connectivity[4] (figure 1).

We've prioritised IT because of its strategic role, growth outlook, and systemic importance to our portfolio. As with all our thematic and idiosyncratic stewardship work, financial materiality remains our primary consideration regarding responsible technology.

- **Strategic role:** IT supports nearly every sector by enabling efficiencies. Adoption is accelerating: **78% of organisations reported using AI in 2024**, up from 55% the previous year[5]. Cloud computing is now considered baseline technology across most sectors[6].
- **Growth outlook:** Worldwide **IT spending is expected to reach US$5.61 trillion in 2025**, up 9.8% from 2024[7]. In the US alone, over 377,000 IT positions are expected to open annually between 2022 and 2032[8].
- **Systemic importance:** As a universal owner, Railpen is exposed to systemic risks and opportunities arising from technological transformation. IT is reshaping the digital landscape, the future of work, energy infrastructure, and the flow of information (page 5).

Our decision to prioritise AI and cybersecurity reflects their rapid and continued evolution, their integration across corporate systems, and the need for robust governance to manage risks and opportunities. AI enables the functionality and intelligence of modern IT ecosystems, while cybersecurity ensures their stability.

Figure 1: **our focus is on information technology**

Technology					
Biotechnology	**Energy technology**	**Manufacturing technology**	**Information technology**	**Transport technology**	**Aerospace technology**

↓

Information technology			
Artificial intelligence	AI is becoming an important enabler of efficiency and innovation, performing tasks that typically require human intelligence, such as learning, reasoning, and decision-making	**Quantum computing**	Quantum computing, while still emerging, has the potential to solve complex problems beyond the reach of classical systems due to its significant processing power
Cybersecurity	Cybersecurity remains critical as the expansion of digital ecosystems increases exposure to risk, making resilience and trust essential	**Cloud and edge computing**	Cloud and edge computing provide the infrastructure needed to support digital transformation and real-time decision-making
		Advanced connectivity	Advanced connectivity, including 5G and Internet of Things (IoT), enables real-time communication between systems for faster, smarter, and more integrated operations

3 University of Cincinnati Online (2024). What is Information Technology?.

4 McKinsey (2025). The Top Trends in Tech 2025.

5 Stanford Institute for Human-Centered AI (2025). AI Index Report 2025.

6 Gartner (2025). Cloud Will Become a Business Necessity by 2028.

7 Ibid.

8 AIPRM (2025). 100+ Technology Statistics 2025.

Key system impacts from IT

Concentration of digital risk

Digitalisation is expanding risk surfaces, while dependence on a small number of hyperscale providers for critical IT services is concentrating risk. This may result in cascading failures across organisations[9].

The future of work

IT continues to augment the way we work, with AI adoption acting as a catalyst for evolving job and skill demands. The International Monetary Fund found that **almost 40% of jobs worldwide are exposed to AI influence**[10] and workforces must be upskilled to take advantage of new technologies.

Related topic: Worth of the Workforce

Energy infrastructure

Emerging IT is simultaneously solving and generating environmental challenges. For example, digitalisation can help integrate the increasing share of renewable power generators and improve the reliability of grids[11]. However, global electricity demand from data centres – a critical part of the infrastructure supporting digitalisation – will double by 2030[12].

Related topic: Climate & Nature

Socio-political dynamics

The security, privacy, and credibility of data flowing through IT is influencing trust in socio-political systems and policymakers' ability to act effectively. Only **40% of people say they trust news**[13], while only one in three citizens trust their government to keep personal data secure[14].

9 CMA (2025). Cloud Services Market Investigation.

10 IMF (2024). AI Will Transform the Global Economy. Let's Make Sure It Benefits Humanity.

11 IEA (2023). Tracking Digitalisation.

12 IEA (2025). Energy Demand from AI.

13 WEF (2023). How can we build trustworthy media ecosystems in the age of AI and declining trust?.

14 Tony Blair Institute for Global Change (2022). Trust in Government: Data, Services and Cover-Ups.

OUR ENGAGEMENT PLAN

Artificial intelligence

AI broadly refers to technologies designed to mimic human thought patterns to solve complex tasks[15]. Its rapid adoption is driving significant and welcome efficiencies and improvements, but also new risks that companies must manage. **In 2024, 72% of companies had adopted AI in at least one business function, but over 60% of S&P companies reported facing material AI-related risks**[16] [17]. While AI offers significant opportunities for businesses and economic growth[a], the rise in AI-related incidents and controversies highlights growing exposure to these risks[18].

Risks emerge across the AI value chain – from intellectual property infringement and litigation over harmful outputs to liabilities from poorly governed AI-driven decisions. Companies also face broader systemic threats, such as resource depletion and heightened cybersecurity vulnerabilities. Although evidence on the financial materiality of these risks is still emerging, our report with Chronos Sustainability 'Achieving Effective AI Governance' illustrates how these risks can translate into financial consequences for portfolio companies[19]. Despite increasing recognition of AI-related risks, governance frameworks[20] remain underdeveloped, and regulatory progress is not keeping pace.

Good governance is fundamental to responsible AI adoption, enabling companies to innovate while managing risks effectively.

Governance across the AI value chain – whether developing or deploying AI systems – is essential for balancing risk and opportunity. Strong oversight, clear accountability and well-defined processes help realise AI's benefits without exposing businesses to undue harm. Governance ultimately turns principles into practice by translating high-level commitments into clear policies, practical frameworks, and actionable processes that guide real-world decisions.

a Our 2025 report 'Achieving effective AI governance' with Chronos Sustainability highlighted several ways in which Railpen is investing across public and private markets in a way which positions the portfolio to benefit from AI opportunities.

Our priority jurisdictions, sectors and engagements

Our engagement priorities are shaped by where Railpen can deliver the greatest impact and create long-term value for our members. This means focusing on companies that combine **material financial exposure**, **systemic importance**, and **opportunities for meaningful change**.

Railpen advances AI governance through **direct company engagement** and **policy advocacy**. We'll prioritise individual corporate dialogue to build expertise and assess companies against our AI Governance Framework. This approach helps identify best practice, improve disclosure and raise governance standards.

15 Information Commissioner's Office (n.d.). Part 1 The basics of explaining AI: Definitions.

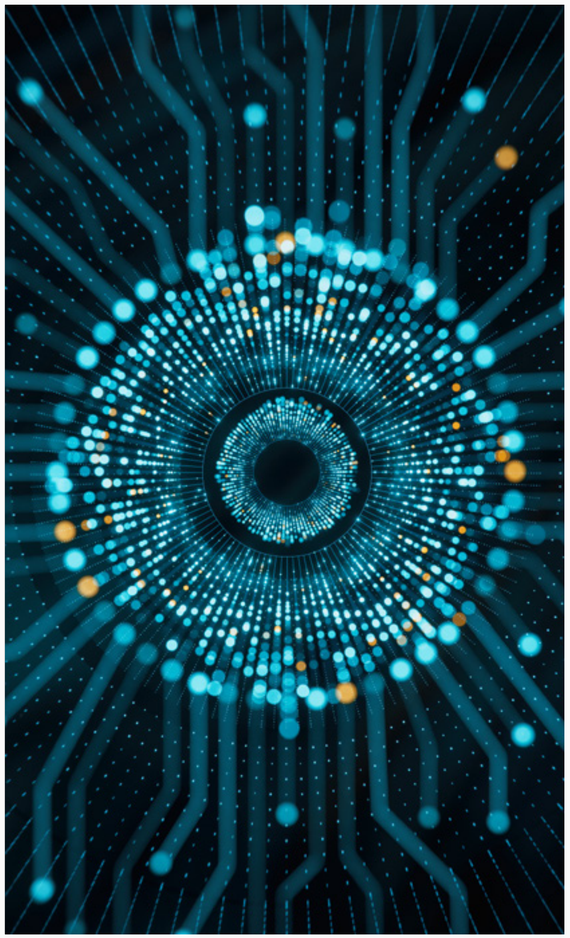
16 McKinsey (2024). The state of AI in early 2024.

17 Deloitte and USC Marshall (2024). Largest Companies View AI as a Risk Multiplier.

18 Stanford Institute for Human-Centered AI (2025). AI Index Report 2025.

19 Railpen and Chronos Sustainability (2025). Achieving effective AI governance.

20 Riskonnect (2023). The New Generation of Risk Report.



Jurisdictions

We'll prioritise jurisdictions where regulatory frameworks and market dynamics create the most material risks and opportunities for long-term investors, and where Railpen has material exposure – the **EU, UK and US**.

The EU's forthcoming AI Act will significantly increase compliance obligations, while all three regions are accelerating AI adoption to safeguard global competitiveness. This pace of innovation brings opportunities but heightens the potential for governance gaps and associated risks.

Sectors

Our engagement strategy prioritises sectors where AI adoption presents the greatest potential for material risk, that are systemically important and where Railpen has material exposures.

High risk sectors include[21]:

- **IT**
- **Financial services**
- **Healthcare**

Financial services and healthcare in particular are foundational to societal and economic stability.

Companies

We aim to engage with companies where AI adoption presents the **highest risk to Railpen's portfolio**, where **systemic ripple effects could be significant**[b], and where our efforts can first identify **leading practices** before informing engagement to drive improved disclosures among lagging peers.

Investor initiatives

Railpen will **prioritise individual company dialogue** over collaborative initiatives, reflecting our focus on governance of AI more widely rather than the specific risks existing collaborative engagement initiatives focus on.

The Investor Alliance for Human Rights and the Cybersecurity Coalition provide platforms for coordinated engagement on digital rights, AI accountability, and cybersecurity resilience. Our participation helps us both work with companies and influence evolving regulatory frameworks.

Policymakers and standard setters

We're prioritising **UK-focused policy advocacy that strengthens AI governance** and seeks to address related systemic risks, such as impacts on the workforce.

This approach leverages Railpen's established relationships with UK policymakers and supports meaningful influence. The UK's current principles-based, 'pro innovation' regulatory stance, alongside the lack of comprehensive AI specific legislation, provides a critical window for shaping balanced, effective regulation.

Our **engagement will target key stakeholders who can embed governance standards across the market**, including government bodies such as the Department for Science, Innovation and Technology (DSIT) and the AI Safety Institute, sectoral regulators like the FCA and ICO, and standard setters. The forthcoming AI Bill may offer a key opportunity for engagement.

b As described in our report, Systemic stewardship: The financially material imperative, Railpen explicitly includes engagement with "systemically important" companies in its systemic stewardship efforts: recognising that positive improvements at 'market-making' or high-profile companies can have a disproportionately beneficial impact in encouraging others in the sector to do likewise.

21 Railpen and Chronos Sustainability (2025). Achieving effective AI governance.

Objectives and milestones

We aim to work with companies to strengthen their AI governance and disclosure, driving alignment with our investor expectations and raising market standards. Our approach includes the following:

- Engaging ESG data providers
- Publishing refined indicators
- Company engagement to gather intelligence and drive change

Success will be reflected in companies' engagement responsiveness, acknowledgement of AI governance materiality, improved scores against our framework, and incorporation of AI governance metrics by data providers.

We'll also advocate for proportionate AI governance mechanisms within UK regulation to ensure systemic resilience and investor confidence. This includes developing our policy position, engaging on forthcoming AI legislation, and influencing regulatory frameworks to embed good standards.

Progress will be measured by regulatory uptake and more consistent AI governance practices.

Cybersecurity

Cybersecurity refers to how individuals and organisations reduce the risk of cyberattacks[22]. Its core function is to protect devices and services from theft or damage. Where this fails, information and system integrity, confidentiality, or availability are jeopardised; and regulation or internal security policies may be violated[23].

Rising incident frequency, cost, and limited organisational preparedness are driving greater cybersecurity risk across investment portfolios.

When incidents occur, companies face major disruption and costly recovery processes, **with average losses reaching an estimated US$4.4 million** in 2024[24]. As described in 'Cybersecurity Risk and Resilience', a 2025 report co-published by Railpen and Royal London Asset Management (RLAM), contributors to this loss can be classified as 'primary' or 'secondary'[25].

Cybersecurity incidents can ripple throughout systems due to technological interdependencies, leading to breakdowns across industries, including those generally considered most vulnerable to cyberattacks: healthcare, manufacturing, finance and insurance, and energy and utilities.

Our priority jurisdictions, sectors and engagements

We focus our engagement where Railpen can have the greatest impact and deliver long-term value for members. We'll continue our partnership with the RLAM-led Cybersecurity Coalition to engage priority companies and promote consistent standards through policy advocacy.

Jurisdictions

We'll target markets with high regulatory activity on cybersecurity, where global cybersecurity standards are set, and are where Railpen's exposure is concentrated – **UK, EU, and US**.

US cybersecurity disclosure requirements are more established, so company engagement can be more impactful in the UK and EU.

Sectors

We will increasingly prioritise companies at the intersection of high-risk exposure and systemic influence:

- **Healthcare:** can have outsized impacts on society and handles protected data
- **Financial services:** critical to economic stability and processes extensive datasets
- **Utilities:** can disrupt operations across sectors and possesses valuable data

This strategy should drive company-level improvements and broader market resilience. Our prioritisation will also take into account sectoral surges in attacks (e.g. consumer retailers in 2025).

22 NCSC (n.d.). What Is Cyber Security?.

23 National Institute of Standards and Technology (2024). Glossary: Cybersecurity Incident.

24 IBM (2025). Cost of a Data Breach Report 2025.

25 FAIR Institute (2020). Primary vs. Secondary Loss in FAIR™ Analysis: What's the Difference and Why It Matters.

Companies

We'll engage with portfolio companies in key jurisdictions, which are **large portfolio holdings, show lagging performance, or face heightened vulnerable from M&A activity or digital transformation.** These present the greatest opportunities for improvement and risk mitigation

We may also engage insurers offering cyber risk transfer solutions – such as Munich Re, AIG, AXA, Hiscox, and Chubb – given their role in shaping cyber risk management expectations for other companies.

Investor initiatives

We plan to continue participating in the **RLAM-led Cybersecurity Coalition** as it's an active platform for collaborative engagement and knowledge-sharing. This will enable us to strengthen governance and resilience at portfolio companies, complementing our individual stewardship efforts where collective action is most effective.

Policymakers and standard setters

We'll prioritise policy advocacy that promotes **harmonised cybersecurity practices and disclosure requirements**, supporting stronger governance, reducing systemic risk, and improving transparency for investors.

Our efforts will **focus on the UK**, where Railpen's proximity to policymakers and industry bodies gives us the greatest opportunity for meaningful influence. While the US already has harmonised requirements and our ability to shape EU policy is limited, we'll monitor global best practice to encourage system-wide alignment. Key stakeholders include the NCSC, DSIT, and standard-setters such as ISO and NIST.

Objectives and milestones

Through collaborative and individual engagement, we aim to strengthen companies' cybersecurity governance and disclosure, driving alignment with our investor expectations for resilient long-term growth and improving preparedness for emerging AI-cyber intersections. Our structured approach – spanning short, medium, and long-term milestones – includes:

- Screening and assessing target companies
- Engaging for change, reviewing progress, and re-engaging where necessary

Success will be reflected in companies' engagement responsiveness, cybersecurity materiality acknowledgement, improved scores against our framework, and incorporation of related expectations into governance practices.

We will also work collectively through the **Cybersecurity Coalition** to raise standards across the market and advocate for regulatory integration of our investor expectations. This includes:

- Publishing refined expectations
- Supporting policy engagement
- Encouraging UK regulators to embed stronger cybersecurity and AI governance requirements

Progress will be measured by improved transparency, regulatory uptake of our principles, and greater consistency in corporate disclosures.

Disclaimer

The information contained in this document is provided solely for informational purposes and has been produced by Railpen Limited. While every effort has been made to ensure the accuracy and completeness of the information, no representations, or warranties (whether express or implied) are made about the completeness, accuracy, reliability, suitability, or availability of the information contained herein. This document does not constitute legal, financial, or professional advice and should not be relied upon as such. Railpen Limited disclaims any and all liability for any loss or damage, whether direct, indirect, consequential, or otherwise, arising from the use or reliance on the information contained herein. The views expressed within this document are those of Railpen Limited at the date of publication, which are subject to change. The information contained within this document does not constitute investment advice and should not be treated as such.

Railpen Limited is a wholly-owned subsidiary of Railways Pension Trustee Company Limited, registered in England and Wales under company number 02315380 whose registered office is at 7 Devonshire Square, London, EC2M 4YH.

7 Devonshire Square, London, EC2M 4YH
SO@railpen.com

RAILPEN