NORTHERN TRUST
ASSET MANAGEMENT

RESEARCH INSIGHTS

STEWARDSHIP IN FOCUS: CYBERSECURITY - RESILIENCE AND GOVERNANCE IN THE AGE OF AI

Our approach

We are advancing our engagement with companies on cybersecurity governance and AI-related cyber risks by assessing oversight, operational resilience, and disclosure practices to support long-term value preservation.

Why it matters

Cybersecurity risks are evolving rapidly as AI adoption, cloud dependency and third-party connectivity expand company exposures, making strong governance, resilience and oversight critical to protecting long-term value creation.

What we've done

Through internal due diligence and company engagement, we have developed expectations for cybersecurity governance, operational resilience, AI-related cyber adaptation and disclosure.

WHY CYBERSECURITY MATTERS TO INVESTORS

Digital transformation is delivering clear business benefits, including greater scalability, faster deployment of services, and deeper integration of data and technology into day-to-day operations. At the same time, it is increasing organizational exposure to cyber threats through increased reliance on interconnected software, third-party providers, cloud environments, digital identities, and emerging artificial intelligence (AI) applications. As a result, cybersecurity is increasingly becoming a business resilience and governance issue with implications for operations, governance, reputation, and long-term value creation.

Cyber incidents can affect operations, customer relationships, regulatory compliance, and long-term value. IBM estimates the global average cost of a data breach at US$4.44 million and the U.S. average at US$10.22 million.[1] Investors increasingly assess a company's ability to prevent, detect, contain, and recover from cyber incidents, particularly as disclosure expectations and

CHIRAG ACHARYA
Sr. Stewardship Analyst, Americas

JOSHUA KENNEDY
Stewardship Analyst, Americas

WATARU TERADA
Stewardship Analyst, Asia-Pacific

[1] Source: IBM. *Cost of a Data Breach Report 2025*. July 30, 2025.

regulatory scrutiny increase. Effective cybersecurity governance therefore serves as an indicator of organizational resilience and risk-management quality.

These figures do not capture every company-specific outcome, but they illustrate that cyber incidents can carry material direct and indirect costs even as detection and containment times improve. For investors, the more relevant point is that financial materiality can arise through a combination of remediation expense, business interruption, legal exposure, and follow-on operational effects.

Operational disruption is equally important. The World Economic Forum's Global Cybersecurity Outlook 2025 highlights the growing complexity of the cyber environment, pressure from third-party dependencies, vulnerability exploitation, credential abuse, and ransomware.[2] In that context, resilience depends not only on preventive controls, but maintaining operational continuity when incidents occur.

Cyber incidents can also create reputational, legal, and disclosure consequences. Companies may need to satisfy breach-notification obligations, respond to regulatory inquiries, preserve evidence, manage litigation or settlement exposure, and disclose material incidents and related impacts in securities filings. The U.S. Security and Exchange Commission's (SEC) final cybersecurity disclosure rule made governance, management processes, and board oversight more visible to investors, reinforcing the relevance of cyber preparedness to stewardship analysis.

OUR STEWARDSHIP APPROACH

As an institutional investor, we assess cybersecurity through the lens of governance, operational resilience, and long-term value preservation. Our stewardship framework incorporates internal due diligence with specific company engagement, recognizing that cyber exposure varies by sector, business model, digital dependency, and the extent to which AI is embedded in operations, products, and services. We focus on whether boards and management can clearly explain how material cyber and AI-related risks are identified, overseen, resourced, tested, and disclosed in practice.

This approach is consistent with NTAM's broader AI stewardship approach, which combines bottom-up, data-driven assessment with targeted engagement and evaluates how companies operationalize AI governance across the business, through cross-functional oversight, transparent risk frameworks, data governance, model controls and responsible deployment, not only whether such policies exist.[3]

Internal Due Diligence. We identify where cyber and AI-related risks may be most material by assessing business-model exposure, digital and third-party dependency, reliance on cloud and identity systems, incident history where

[2] Source: The World Economic Forum. *Global Cybersecurity Outlook 2025*. January 13, 2025.
[3] Source: Northern Trust Asset Management. *Stewardship in Focus: Artificial Intelligence*. 2025.

relevant, and the extent to which cyber risk is integrated into enterprise risk management. Where AI adoption is relevant, we also assess whether companies have defined governance processes for data, models, access, monitoring, and escalation.

Company Engagement. Engagement with boards and management helps us understand how governance operates in practice. We focus on accountability at the management level, how information is escalated to the board, whether oversight responsibilities are clearly defined, and how resilience, incident preparedness, and disclosure quality are evaluated. We also assess whether cyber risk is discussed in business terms, including operational continuity, customer trust, legal exposure, and capital allocation.

AI-Related Cyber Adaptation. As AI becomes more embedded in business processes, we assess how companies are adapting cybersecurity programs to address risks such as data leakage, weak model access controls, unsanctioned or shadow AI, third-party model dependence, insecure integrations, and employee misuse. We also evaluate how companies train employees, test controls, and incorporate AI-related scenarios into incident response and resilience planning. This practice is focused on assessing how a company is evolving its cybersecurity program and governance practices to address the unique risks introduced by AI adoption.

CYBERSECURITY IN THE AGE OF AI

Cybersecurity is increasingly relevant to how investors think about resilience, operational continuity, and long-term value protection as companies become more digitally dependent. AI adds to that relevance because it can strengthen cyber defensive capabilities, but it can also expand the ability for evolved attacks, increase reliance on data and third parties, and be used by attackers in phishing and deepfake impersonation campaigns. Agentic AI models may further increase cyber risk by accelerating the discovery of software vulnerabilities, lowering barriers to sophisticated attacks, and creating new challenges around oversight of autonomous agents. IBM reported that 16% of the breaches it studied involved attackers using AI tools, and that among organizations that experienced an AI-related security incident, 97% lacked AI access controls.[4]

Regulatory and policy attention is also increasing. In the U.S., Executive Order 14409, issued on June 2, 2026, frames advanced AI as both an innovation and a national security issue, directs agencies to strengthen cyber defenses, and establishes a voluntary framework for collaboration with AI companies and critical infrastructure operators.[5] More broadly, the SEC's cyber disclosure rules and evolving resilience focused frameworks across major markets indicate that governance expectations are becoming more explicit. For investors, this does not eliminate the need for case-by-case analysis, but it does heighten the importance

[4] Source: IBM, *"13% Of Organizations Reported Breaches Of AI Models Or Applications, 97% Of Which Reported Lacking Proper AI Access Controls,"* Press Release. July 30, 2025

[5] Source: The White House, "Executive Order 14409: PROMOTING ADVANCED ARTIFICAL INTELLIGENCE INNOVATION AND SECURITY." June 2, 2026.

of understanding how companies govern AI related cyber risk before incidents occur. In Europe, recent regulatory developments have similarly moved cybersecurity further into mainstream risk management and governance, while AI-specific measures reinforce the importance of oversight as AI becomes more embedded in products, services and operations. These regulatory shifts are accompanied by emerging complexities around agentic AI, where agent identity, delegated authority, and monitoring for anomalous or rogue behavior are becoming critical areas of protection. OpenAI's GPT 5.6 Sol is a confirmed frontier model with capabilities relevant to cybersecurity and agentic workflows. Anthropic's Mythos model has been referenced in benchmark comparisons and external reporting, though it is less clearly documented in primary company disclosures. More broadly, the security landscape for agentic AI remains fragmented, and capabilities for identity, governance, and real time monitoring are still developing.

The most relevant risks and rising expectations will differ by business model and sector. Companies that develop AI systems, software, or cloud services may face closer scrutiny over model security, data integrity, testing, and vulnerability management. Companies in sectors where a cyber disruption could quickly interrupt essential services, payments, communications, healthcare, logistics, or physical operations may face particularly high expectations around resilience, third-party oversight, and recovery readiness. The healthcare industry continues to be at the forefront of risk as reliance on outdated systems, massive stores of confidential information, and underinvestment in cybersecurity culminate a breeding ground for bad actors and attacks.[6] From a stewardship perspective, this reinforces the importance of a risk-based approach rather than a one-size-fits-all checklist.

EXPECTATIONS FOR CYBERSECURITY GOVERNANCE

Governance. We believe cybersecurity governance should be treated as a board-level responsibility embedded in enterprise risk management, not as a stand-alone technical function. From an investor stewardship perspective, the central question is whether oversight is clear, credible, and proportionate to the company's risk profile. Key questions we ask: where responsibility sits at the board level; who in management is accountable; how cyber issues are escalated; and how cyber risk is weighed alongside other enterprise risks. Where AI is highly material, these questions should extend to whether the board and management have access to appropriate AI expertise; whether accountability for AI oversight is clearly assigned through cross-functional governance structures; and whether AI-related cyber risks are addressed through transparent risk frameworks, data governance, model controls and regular board escalation.[7] Gartner's forecasts help explain why this is now a strategic governance issue rather than a peripheral IT concern: it projects worldwide end-user spending on information security to reach US$213 billion in 2025, while overall IT spending is

[6] Source: ACSMI. *Data Breach Report: Industries at Risk and Mitigation Strategy*. July 14, 2025
[7] Source: Northern Trust Asset Management. *Stewardship in Focus: Artificial Intelligence*. 2025.

expected to grow 7.9% in the same year, underscoring that cybersecurity is increasingly being treated as a strategic investment rather than a routine technology expense.[8]

Resilience. Effective cyber governance is demonstrated by clear accountability, board-level oversight, tested incident response, and resilience planning that is integrated into enterprise decision-making. We expect companies to explain how incident response plans are tested, how business continuity and recovery readiness are assessed, how lessons learned are incorporated after incidents, and how critical third-party, software, identity, and cloud dependencies are governed. This does not require a single committee structure or disclosure of sensitive technical detail, but it does require evidence that cyber oversight is integrated into broader enterprise decision-making and that resilience is managed as an operational and strategic priority. Industry research notes that security software is the fastest-growing segment of security spending as organizations continue moving from on-premises to cloud-based systems.[9] Additional reports emphasize that resilience depends on regularly testing incident response plans and backups, defining clear roles, conducting crisis simulations, and maintaining core data-security disciplines such as discovery, classification, access control, encryption, and key management.[10]

AI Governance. AI makes these governance expectations more urgent as it enhances enterprise-wide risks that requires boards to provide clear oversight, accountability, transparency, and risk management at a pace traditional governance structures were not designed to handle. IBM's report identifies that a majority of the organizations that reported breaches lacked an AI governance policy or were still developing one.[11] In practice, our assessment considers whether a company maintains appropriate governance over model inventories, permissions, access to sensitive data, prompt and data leakage risks, shadow or unsanctioned AI use, third-party AI tools, and employee training. We also consider whether the company provides clarity on how AI-related scenarios are incorporated into cyber resilience planning. IBM further reports that one in five organizations experienced a breach due to shadow AI, while organizations using AI and automation extensively in security operations saved an average of US$1.9 million in breach costs and reduced breach lifecycles by 80 days,[12] reinforcing that AI governance is a practical resilience issue rather than a speculative one. These AI-specific cyber expectations are consistent with NTAM's broader AI stewardship framework, which emphasizes board and management accountability, cross-functional oversight, transparent AI risk frameworks, data governance, model controls, and responsible deployment. For

[8] Source: Gartner, "*Gartner Forecasts Worldwide End-User Spending on Information Security to Total $213 Billion in 2025,*" Press Release. July 29, 2025.
[9] *Ibid*
[10] Source: The Business Continuity Institute. *BCI Continuity and Resilience Report 2025*. September 24, 2025.
[11] Source: IBM. *Cost of a Data Breach Report 2025*. July 30, 2025.
[12] *Ibid*

a broader discussion, see Northern Trust Asset Management's Stewardship in Focus: Artificial Intelligence.[13]

Disclosure. Disclosure quality remains central to investor assessment. The strongest disclosure enables investors to understand how cyber governance is structured, how management accountability and escalation work in practice, how incidents are assessed for materiality, how resilience is tested, and how third-party and AI-related exposures are monitored without revealing operationally sensitive detail. The objective is not to prescribe a single governance architecture; it is to assess whether cyber governance appears integrated, accountable, and responsive to a threat environment shaped by cloud dependence, ecosystem interconnection, and the accelerating use of AI.

CONCLUSION

Cybersecurity is a useful indicator of broader organizational quality, including governance discipline, operational resilience, risk culture, and the ability to manage complexity across a networked enterprise. As AI adoption, third-party dependencies, and disclosure expectations continue to evolve, our stewardship analysis focuses on whether companies identify, govern, and manage cyber risk effectively. We believe boards and management teams should strive to eliminate as many cyber risks as possible, but are aware it's unlikely risks can be entirely eliminated. Therefore, understanding the mitigation and response plan is critical in order to demonstrate that material risks are understood, governance is clear, resilience is tested, accountability is defined, and disclosure helps investors evaluate whether the company is adapting appropriately as technology and threats evolve.

[13] Source: Northern Trust Asset Management. *Stewardship in Focus: Artificial Intelligence*. 2025.

NORTHERN TRUST ASSET MANAGEMENT
ntam.northerntrust.com

IMPORTANT INFORMATION

For Asia-Pacific (APAC) and Europe, Middle East and Africa (EMEA) markets, this information is directed to institutional, professional and wholesale clients or investors only and should not be relied upon by retail clients or investors.

Northern Trust Asset Management is composed of Northern Trust Investments, Inc., Northern Trust Global Investments Limited, Northern Trust Fund Managers (Ireland) Limited, Northern Trust Global Investments Japan, K.K., NT Global Advisors, Inc., 50 South Capital Advisors, LLC, Northern Trust Asset Management Australia Pty Ltd, and investment personnel of The Northern Trust Company, The Northern Trust Company (Singapore Branch), and The Northern Trust Company of Hong Kong Limited.

Issued in the United Kingdom by Northern Trust Global Investments Limited, regulated by the Financial Conduct Authority (License Number 191916); issued in the European Economic Area (EEA) by Northern Trust Fund Managers (Ireland) Limited, regulated by the Central Bank of Ireland (License Number C21810); issued in Australia by Northern Trust Asset Management (Australia) Limited (ACN 648 476 019), which holds an Australian Financial Services Licence (License Number 529895) and is regulated by the Australian Securities and Investments Commission (ASIC); issued in Hong Kong by The Northern Trust Company of Hong Kong Limited, which is regulated by the Hong Kong Securities and Futures Commission; and issued in Singapore by The Northern Trust Company (Singapore Branch), which is regulated by the Monetary Authority of Singapore.

This information is directed to institutional, professional and wholesale current or prospective clients or investors only and should not be relied upon by retail clients or investors. This document may not be edited, altered, revised, paraphrased, or otherwise modified without the prior written permission of NTAM. The information is not intended for distribution or use by any person in any jurisdiction where such distribution would be contrary to local law or regulation. NTAM may have positions in and may effect transactions in the markets, contracts and related investments different than described in this information. This information is obtained from sources believed to be reliable, its accuracy and completeness are not guaranteed, and is subject to change. Information does not constitute a recommendation of any investment strategy, is not intended as investment advice and does not take into account all the circumstances of each investor.

This report is provided for informational purposes only and is not intended to be, and should not be construed as, an offer, solicitation or recommendation with respect to any transaction and should not be treated as legal advice, investment advice or tax advice. Recipients should not rely upon this information as a substitute for obtaining specific legal or tax advice from their own professional legal or tax advisors. References to specific securities and their issuers are for illustrative purposes only and are not intended and should not be interpreted as recommendations to purchase or sell such securities. Indices and trademarks are the property of their respective owners. Information is subject to change based on market or other conditions.

All securities investing and trading activities risk the loss of capital. Each portfolio is subject to substantial risks including market risks, strategy risks, advisor risk, and risks with respect to its investment in other structures. There can be no assurance that any portfolio investment objectives will be achieved, or that any investment will achieve profits or avoid incurring substantial losses. No investment strategy or risk management technique can guarantee returns or eliminate risk in any market environment. Risk controls and models do not promise any level of performance or guarantee against loss of principal. Any discussion of risk management is intended to describe NTAM's efforts to monitor and manage risk but does not imply low risk.

Past performance is not a guarantee of future results. Performance returns and the principal value of an investment will fluctuate. Performance returns contained herein are subject to revision by NTAM. Comparative indices shown are provided as an indication of the performance of a particular segment of the capital markets and/or alternative strategies in general. Index performance returns do not reflect any management fees, transaction costs or expenses. It is not possible to invest directly in any index. Net performance returns are reduced by investment management fees and other expenses relating to the management of the account. Gross performance returns contained herein include reinvestment of dividends and other earnings, transaction costs, and all fees and expenses other than investment management fees, unless indicated otherwise. For U.S. NTI prospects or clients, please refer to Part 2a of the Form ADV or consult an NTI representative for additional information on fees.

Forward-looking statements and assumptions are NTAM's current estimates or expectations of future events or future results based upon proprietary research and should not be construed as an estimate or promise of results that a portfolio may achieve. Actual results could differ materially from the results indicated by this information.

NOT FDIC INSURED | MAY LOSE VALUE | NO BANK GUARANTEE