持続可能で強靭な投資のためのサイバーセキュリティ評価のESG・信用リスク分析への統合

野村アセットマネジメント
債券サステナブル・インベストメント・ヘッド
ジェイソン・モーティマー

▌要　約 ▐

1. 次世代 ESG 投資インテグレーションのためのサイバーセキュリティと現実世界への影響：環境・社会・ガバナンス（ESG）投資インテグレーションは、重要な社会経済的・環境的課題にも対処する方法でリスク調整後リターンを改善するために、市場における重要かつ非財務要因を考慮することを指す。投資分析における企業の温室効果ガス排出データの統合は、このプロセスの主要な例である。サイバーセキュリティは現在、金融及び投資リスクとの強い結びつき、規制当局による監視の強化及び現実世界への影響の可能性を背景に、主要な投資家にとって主要な次世代 ESG 要因として浮上している。本稿は、このような傾向を考察すると共に、リスク管理と企業エンゲージメントのため社債の ESG 投資プロセスにサイバーセキュリティリスクを統合する野村アセットマネジメント（NAM）のアプローチを紹介する。
2. 増大する企業のサイバーセキュリティリスクの財務的な重要性と規制対応：投資家は、社債投資ポートフォリオに内在する潜在的なサイバーセキュリティリスクを評価することに関心を高めている。経済のデジタル化によって、ハッカーが悪用できるサイバー攻撃の対象領域が拡大するにつれて、企業のサイバー攻撃は深刻さと頻度を増している。また、サイバー空間における不十分な保護は全体的な経済成長と国家の安全保障を脅かしており、サイバー犯罪による世界の損失額は 2021 年には 6 兆米ドルと推計されている。このような状況を踏まえ、世界のビジネスリーダーや政治リーダーを対象とした調査では、サイバーセキュリティがその影響と可能性から、気候変動や地政学的紛争と並んで世界的なリスクのトップに挙げられている。世界のサイバーセキュリティ規制をめぐっては、重要なインフラと必要不可欠なサービスの保護に焦点を当てて、企業のサイバーセキュリティにおけるパフォーマンスに関する厳格な開示をさらに義務付けるとみられる。
3. クレジットの ESG 分析にサイバーセキュリティデータを統合する NAM のアプローチ：サイバーセキュリティの悪影響の拡大と社会における認識の高まりにより、投資家はこのトピックを投資調査や企業のエンゲージメントに統合するようになっている。NAM では、サイバーセキュリティの投資における重要性を認識しており、企業の信用力分析でサイバーリスクを体系的かつ定量的に測定するための独自のアプローチを開発した。各種データを使用して、ソフトウェアの脆弱性への定期的な修正・更新や、データとネットワークのセキュリティ確保のためのベストプラクティスの適用など、投資先企業が優れた「サイバー上の衛生管理」を実践している度合いを分析している。その上で、企業のサイバーセキュリティリスクとパフォーマンスのデータは、NAM のグローバル債券投資戦略に統合された独自のクレジット ESG スコアリングモデルにおいて、ガバナンス要因として直接組み込まれる。
4. NAM では今後も、サイバーセキュリティを ESG 投資のトピックとして取り上げることで、企業のサイバーセキュリティに関するパフォーマンス基準の向上にインセンティブを与え、社会経済の回復力に貢献して現実世界にプラスの影響をもたらし、潜在的に顧客の社債投資のリスク調整後リターンを向上させたいと考えている。

Ⅰ　次世代 ESG 投資インテグレーションのためのサイバーセキュリティと現実世界への影響

環境・社会・ガバナンス（ESG）インテグレーションとは、実務的な観点に基づくと、重要な社会経済や環境課題にも対応する方法を取りながら投資のリスク調整後リターンを改善するために、投資分析において市場の重要な非財務情報を考慮することである。炭素排出量と気候変動は、ESG リスクに対する認識と市場価格形成の変化が現実世界にどのように影響を与えるかを示す代表的な例として挙げられる。例えば、今日では投資家が温室効果ガス（GHG）排出量の開示を投資プロセスに組み込むことは、主流の慣行となっている。その結果、企業の炭素パフォーマンスに対する投資家の認識に応じて、数兆米ドルの資本が配分され、価格設定されている。このような企業のリスクと評価の再設定により、企業は地球規模の気候変動緩和の取り組みを支援するために、排出削減を推進する強力なインセンティブを持つようになった。従って、投資家は、以前は評価されていなかった外部不経済である「市場の失敗」に対処することで、現実世界への影響を達成し、投資リスクを回避できる。

つまり、投資家は、市場価格に重大な影響を与え、追加の規制リスクを引き寄せる可能性のあるグローバルな課題に関連した新たな非財務的な ESG 要因を特定するインセンティブを得ることができる。そのような中、サイバーセキュリティは、財務リスクや投資リスクとの強い関連性、規制当局による監視の強化、現実世界に影響を与える可能性などから、多くの投資家にとって主要な次世代の ESG 課題として浮上している。

本稿は、企業のサイバーセキュリティリスクの財務上の重要性を分析し、世界的な規制動向の傾向を探るとともに、リスク管理と企業エンゲージメントのため社債の ESG 投資プロセスにサイバーセキュリティリスクを組み込む野村アセットマネジメント（NAM）のアプローチを紹介する。

Ⅱ　企業のサイバーセキュリティリスクの財務的重要性－ミクロ経済（企業）コスト

投資家は、社債投資ポートフォリオに内在する潜在的なサイバーセキュリティリスクを評価することに対して関心を高めている。サイバー犯罪は、データ侵害とランサムウェア攻撃の頻度の増加、企業のサイバー防御と保険への支出の増加、風評被害を通じて、個々の企業に影響を与えている。大規模なサイバー攻撃は、業務やビジネスに混乱を引き起こし、重大な訴訟リスクを発生させる可能性がある。

経済のデジタル化により、ハッカーが悪用するサイバー「攻撃対象領域」が拡大するにつれて、サイバー犯罪の発生率と頻度が増加している。企業あたりのサイバー攻撃率の推定値は、2020 年から 2021 年にかけて 31%増加し[1]、2022 年の個々のデータ侵害の平均コストは 435 万米ドルに上昇している[2]。ランサムウェアは企業にとって大きな懸念事項と

[1] Accenture, “State of Cybersecurity Resilience 2021,” 2021.
[2] IBM, “Cost of a Data Breach 2022 Report,” July 2022.

なっており、IBM の調査データによると、全体の 83%の組織が過去 2 年間にランサムウェア攻撃を経験したことが示されている[3]。現在、米国企業で最も一般的に要求される身代金額は、500 万ドルから 1,000 万ドルの範囲にある。企業のサイバー防護と保険への支出は、企業にとって大きなコストとして浮上している。

サイバーセキュリティ関連の製品やサービスに対する企業支出の全体規模は、2017 年から 2021 年までの 1.0 兆米ドルに比して、2021 年から 2025 年の 5 年間には 1.75 兆米ドルに達すると推計されている[4]。特定の米国金融機関は、デジタルインフラ及び顧客情報のセキュリティと保護のみに年間 10 億米ドル以上を費やしていると報告されているが、これは重要なセクターにおけるサイバー関連の支出が膨大な規模であることを示唆している。サイバー保険を選択する企業が増加しており、米国のある調査では、保険加入率が 2016 年の 26%から 2020 年には 47%に上昇した[5]。サイバー保険料は 2021 年に約 3～4 割上昇しており、サイバー保険の市場規模は 2021 年の約 85 億米ドルから 2031 年までに 340 億ドルに成長すると予測されている。

最近の大規模なサイバー攻撃は、病院や製薬会社[6]、旅行とレジャー会社[7]、金融サービス[8]、エネルギーインフラ事業者[9]を標的にしている。個々の攻撃は、業務に支障をきたし、何億ドルもの事業損失や法的責任をもたらすだけでなく、機密性の高い個人情報を危険にさらし、国家の重要機能を脅かす可能性がある。2017 年に注目を集めた事例では、中国の軍事ハッカー[10]が、パッチが適用されていないソフトウェアの脆弱性を悪用し、消費者信用調査機関に侵入した。国を後ろ盾にした同サイバー攻撃者により、約 1 億 4,500 万人の氏名や住所、社会保障番号などの個人を特定できる情報をはじめとする詳細な財務記録が盗み出された。同社がデータ侵害を開示したとき、同社の株価は最大で 35%近く下落し、投資適格級の社債のクレジット・スプレッドは 118 ベーシスポイント（bp）拡大した。2019 年に、同社は米国の連邦取引委員会（FTC）と、少なくとも 5 億 7,500 万米ドルもの罰金、罰則及び消費者の賠償について和解に達した。

Ⅲ 企業のサイバーセキュリティリスクの財務的重要性ーマクロ経済的コスト

より広い社会全体の視点で、サイバースペースでの不適切な保護は、国家戦略に影響を与えるマクロ経済的な損害につながる可能性がある。これらの影響には、大規模な産業ス

[3] IBM, “Cyber Resilient Organization Study 2021,” 2021.
[4] David Braue, “Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025,” *Cybercrime Magazine*, September 10, 2021.
[5] U.S. Government Accountability Office, “Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market,” May 20, 2021.
[6] David Voreacos, Katherine Chiglinsky, Riley Griffin, “Merck Cyberattack’s $1.3 Billion Question: Was It an Act of War?,” *Bloomberg*, December 3, 2019.
[7] “Marriott Hacking Exposes Data of Up to 500 million Guests,” *The New York Times*, November 30, 2018.
[8] Federal Trade Commission, “Equifax Data Breach Settlement,” September 2022.
[9] “The Colonial Pipeline Hack is a New Extreme for Ransomware,” *WIRED*, May 8, 2021.
[10] Federal Bureau of Investigation, “Chinese Military Hackers Charged in Equifax Breach,” February 10, 2020.

パイ活動やイノベーション及び投資のインセンティブの低下、個人情報のプライバシーの侵害による間接的な経済的損失が含まれる。また、経済と国家安全保障、公衆衛生、市民の安全と自由を支える重要機能とインフラに対する脅威も含まれる。投資家は、サイバーセキュリティによるリスクは直接影響を受ける企業に留まらず、経済と市場の評価を支える社会全体にまで及ぶことをますます意識している。

サイバー犯罪とサイバースパイ活動による経済的損害は、計り知れない規模で拡大している。サイバー犯罪による世界の年間損失額は、2021 年の 6 兆ドルから 2025 年まで 10.5 兆ドルに達する可能性を指摘する情報筋もある[11]。これとは対照的に、2021 年の再保険会社の報告[12]によると、気候変動による経済的損失は 2050 年までに累計 23 兆ドルに達すると推定される[13]。方法論[14]と統計サンプリング[15]の違いにより、これらの数値を直接比較することは困難だが、サイバーセキュリティの経済的影響は、地球規模の気候変動と同程度の規模になる可能性があることが示唆されている。これを反映して、サイバーセキュリティは、気候変動と地政学的紛争とともに、世界の最高経営責任者（CEO）[16]と意思決定者[17]の認識調査で一貫して地球規模のリスクの上位 5 位に位置する。

サイバー攻撃の標的となることが最も多いセクターは、金融、ヘルスケア、情報技術及び製造業[18]であり、新型コロナウイルス感染症のパンデミック中はヘルス及び製薬セクターを標的とするサイバー犯罪が特に増加した。これらのセクターは、金銭的動機のあるサイバー犯罪者に高額な金銭的ターゲットを提供するだけでなく、国家を後ろ盾とするサイバー攻撃者にとって、混乱や破壊された場合に高い戦略的価値を持つ重要な国家機能にも関連している。また、これらのセクターは、金銭的および地政学的な動機を持つハッカーにとって魅力的なターゲットである非有形の知的財産を多く所有する傾向がある。2013 年、米国国家安全保障局（NSA）の高官は、サイバースパイ活動を「史上最大の富の移転」[19]と表現した。

市場参加者は、脆弱な企業のサイバーセキュリティによる直接的および間接的なコストの増大をますます意識している。この傾向に基づき、サイバーセキュリティのパフォーマンスを非財務（ESG）要因として企業投資の分析に取り入れ始める投資家が増加している。

11 “2022 Cybersecurity Almanac,” *Cybercrime Magazine*, January 19, 2022.
12 Swiss Re Group, “Climate Action – This is a Mission Possible,” November 3, 2021.
13 “Climate Change Could Cut World Economy by $23 Trillion in 2050, Insurance Giant Warns,” *The New York Times*, April 22, 2021.
14 Organisation for Economic Co-operation and Development, “Losses and Damages from Climate Change.”
15 Dinei Florencio and Cormac Herley, “Sex, Lies and Cyber-Crime Surveys,” *Microsoft Research*, June 2011.
16 PWC, “PwC 25th Annual Global CEO Survey Reimagining the outcomes that matter,” January 17, 2022
17 World Economic Forum, “These are the Biggest Global Risks,” January 16, 2019.
18 Statista, “Global Industry Sectors Most Targeted by Basic Web Application Attacks from November 2020 to October 2021,” May 2022.
19 Infosec, “Cyber-Espionage: The Greatest Transfer of Wealth in History,” February 12, 2013.

Ⅳ 最近のサイバーセキュリティの世界的な規制動向の概要

機関投資家は、急速に変化するサイバーセキュリティの規制環境に直面している。地政学的な競争が激化する中でサイバーセキュリティが社会に与えるコストは増大しており、世界中の政府の 80%がサイバー犯罪法と情報保護法[20]を制定するなど、世界の政策担当者にとってサイバーセキュリティはますます重要なトピックとなっている。米国や欧州連合（EU）、英国、日本では、サイバーセキュリティ法の改訂及び追加が進んでおり、重要なインフラと不可欠なサービスに対する規制の監視や開示要件、適用範囲が拡大する傾向にある。

１．米国

FTC や証券取引委員会（SEC）、米国サイバーセキュリティ・社会基盤安全保障庁（CISA）はすべて、2022 年に国家レベルの新しい規制を提案している。米国におけるサイバーセキュリティ規制の新たな焦点は、サイバー侵害の報告、サプライチェーンのサイバーセキュリティに係るコンプライアンス、消費者情報の損失につながる既知のソフトウェアの脆弱性にパッチを適用しなかった企業に対する法的責任の可能性などに焦点を当てている。2022 年前半、米国の 24 の州が新たなサイバーセキュリティ法を制定し[21]、その主な焦点は、サイバーセキュリティ基準の設定、公共部門のサイバーセキュリティプログラムへの資金提供の増加、サイバーセキュリティの一般労働者のトレーニング、選挙・投票システムの完全性強化に置かれている。

２．EU

EU において、主要なサイバー関連の規制は主に消費者保護に焦点を当てている。個人情報とオンラインプライバシーの取り扱いと管理を扱う画期的な欧州連合（EU）一般データ保護規則（GDPR）が 2016 年に施行された。2022 年には、欧州サイバーレジリエンス法案[22]が策定され、EU で販売されるハードウェア及びソフトウェア製品の製品寿命全体にサイバーセキュリティ要件を課すことが提案された。また、EU では最近、更新されたネットワーク及び情報システム指令（NIS2 指令）[23]が、重要なインフラ保護に重点を置き、インシデント管理及び報告義務[24]を更新した上で、EU における耐障害性とインシデント対応能力を向上させる一連の措置として、可決された。

---

[20] United Nations Conference on Trade and Development, “Global Cyberlaw Tracker.” ＜https://unctad.org/page/cyberlaw-tracker-country-detail、2022 年 10 月 10 日閲覧＞

[21] National Conference of State Legislatures, “Cybersecurity Legislation 2021,” July 1, 2022.

[22] European Commission, “Cyber Resilience Act – Factsheet,” September 15, 2022.

[23] European Commission, “NIS Directive.” ＜https://digital-strategy.ec.europa.eu/en/policies/nis-directive、2022 年 6 月 7 日閲覧＞

[24] European Council, “Strengthening EU-Wide Cybersecurity and Resilience – Provisional Agreement by the Council and the European Parliament,” May 13, 2022.

３．英国

英国の EU 離脱（ブレグジット）後の一般データ保護規則（UK-GDPR）は、GDPR[25]と同様に主要な原則と権利、義務を保持している。2018 年に可決されたネットワーク及び情報システムのセキュリティ規則（NIS 規則）は、情報ネットワークのサイバーレジリエンスと重要なサービスのための重要な国家インフラを強化するための法的措置である。英国政府は現在、民間産業にインセンティブを与えて、サイバーセキュリティへの投資を増やすためのオプションを検討している。このテーマに関する最初の白書では、変化するリスク環境[26]の中でより良い慣行をより迅速に確立するためには、市場インセンティブとより介入的な規制が必要になる可能性があることが認識されている。

４．日本

日本のサイバーセキュリティに関する規制と法律は、他の先進国市場に比べて比較的遅れていると見られている。サイバーセキュリティ基本法は、日本のサイバーセキュリティに関する基礎的な法律であり、個人情報保護法（APPI）は情報保護に関する日本の主要な法律である。2022 年の APPI の改正では、個人情報侵害の場合における報告と通知が義務付けられているが、これまでのところ、その他の場合のサイバー侵害報告の義務はない。また、日本には現在、安全なソフトウェア開発に関する具体的な規制がない。米国や EU、英国の動向を反映して、日本政府は現在、疑わしい通信を監視および分析するためのネットワークシステムへの政府アクセスを許可する、重要なインフラをカバーするアクティブサイバーディフェンス（ACD）の枠組みの導入を検討している[27]。

V　NAM の信用力分析・エンゲージメントにおけるサイバーセキュリティへの取り組み

企業や社会に対する悪影響の拡大とリスクの増大、サイバーセキュリティリスクとその悪影響に対する一般の意識の高まり、規制強化による政治的監視の高まりはすべて、資産運用会社にサイバーセキュリティが広く採用されるよう後押しする要因である。投資家にとってサイバーセキュリティの重要性が高まっており、NAM は、サイバーセキュリティを体系的かつ定量的に信用力分析に組み込む独自のアプローチを開発した。

１．「市場の失敗」としてのサイバーセキュリティリスクの理解

NAM ではサイバーセキュリティを統合構築する最初のステップとして、企業のサイ

[25] Information Commissioner's Office, "The UK GDPR."
[26] Government Digital Service, "2022 Cyber Security Incentives and Regulation Review," January 19, 2022.
[27] "Active cyber defense framework could one day protect Japan," *The Japan News*, September 13, 2022.

バーセキュリティリスクを効果的に認識、評価、価格設定するために市場が直面している現在の課題を検討した。

第一に、従来の企業のサイバーセキュリティは、IT 部門の延長として扱われてきた。この傾向により、多くの企業はサイバーセキュリティの準備と復元力を、優れたオペレーション運営の源としてではなく、最小限に抑えるべきコンプライアンスコストと見なすようになっている。その結果、サイバーセキュリティ対策への支出は、リスクのレベルに比べて不十分であることが多い。企業のサイバーセキュリティの指揮命令系統や責任はしばしば不明確であり、このテーマに関する取締役会の監督と専門知識は限られている。企業におけるサイバーセキュリティの優先順位付が不十分であることが、今日見られる専門知識と人材の不足の一因となっている。従って、投資家と企業経営者の間でサイバーセキュリティの地位をより戦略的な実務およびビジネスレベルに引き上げ、必要なレベルの投資を約束し、市場の需要を満たすためにサイバーセキュリティの専門家の十分な人材を開発することが重要である。

第二に、サイバーセキュリティは一般的に法律や規制の範囲外に存在している。ほとんどのデジタルインフラは個人所有であるため、サイバーセキュリティポリシーは通常、規制要件ではなく「ベストプラクティス」に基づいている。これにより、サイバーセキュリティの実装は、政府や投資家からの十分な監視なしに、企業内の機能として残されている。ほとんどのサイバー事件と違反は、公に報告または認知されていないため、投資家がサイバーセキュリティリスクを評価することが困難となる。特に法的な要件がない場合に、企業がサイバー事件を開示することによる羞恥や潜在的な追加のコストを避けたいと考えるため、こうした状況は理解に難しくない。今後、投資分析におけるサイバーセキュリティリスクの体系的な組み込みにより、より重要なサイバーセキュリティ関連の開示に対する需要が生まれる。同時に、サイバーセキュリティ規制の更新により、違反の開示がさらに求められ、特に重要なインフラと不可欠なサービスにおいて、サイバーセキュリティへの備えを強化することが義務付けられる。

第三に、企業のサイバーセキュリティリスクに効果的に対処するための「万能」なアプローチはない。企業全体でサイバーセキュリティのパフォーマンスの評価を標準化することは容易ではない。サイバー犯罪者は、さまざまな侵入戦略を用いて日和見的に弱点領域を標的にしているため、リスクベクトルと攻撃方法は常に変化している。つまり、サイバーセキュリティの防御者は、リスクの高い特定のシステムやプロセスだけに焦点を当てたり、単一の防御方法に依存することはできないということである。ひいては、投資家は、既知の弱点の比較評価に基づいて企業間の特有なサイバーセキュリティリスクを評価する一般的な枠組みを使用することはできない。また、他の犯罪と同様に、サイバー犯罪の予測は不可能ではないにせよ、困難である。通常、企業はサイバーセキュリティのポリシーとパフォーマンスに関する有意な詳細を一般投資家に開示することはなく、サイバーの脆弱性に関する過剰な情報開示は、より多くのサイバー攻撃を引き付けるだけであるという正当な懸念がある。このことから、投資家が企業全体のサイバーセキュリティを評価する

際には、サイバーセキュリティリスクの代用として、サイバーセキュリティへの準備とベストプラクティスの遵守による事前の対策に頼らざるを得ないことが予測される。

これらの課題により、投資家がサイバーセキュリティリスクを投資プロセスに包括的に組み込むことが困難になっている。特に、比較可能なサイバーセキュリティの実績に関する情報やその測定方法が不足していることにより、市場は企業のサイバーセキュリティリスクを効率的に評価することができなかった。市場からの圧力がなく、今のところ規制要件も限られているため、企業は自社のサイバーセキュリティへの投資が不足する傾向にあり、その結果、サイバー攻撃を受ける可能性が他のケースよりも高くなる。しかし、サイバーセキュリティ保護への投資不足による被害は、顧客や国民、社会全体にも及ぶ。言い換えれば、サイバーセキュリティリスクの体系的な過小評価は、炭素排出や産業公害・廃棄物によって引き起こされる外部不経済と同様に、市場の失敗を意味する。

２．NAM が次世代の ESG 要因としてサイバーセキュリティデータをどのように採用したか

社債投資におけるサイバーセキュリティリスクの評価と統合という課題に効果的かつ包括的に対処するために、NAM では「サイバーセキュリティ・ハイジーン（サイバー上の衛生管理）」の体系的な測定に重点を置いている。このサイバー衛生は、既知の脆弱性に対する定期的なプログラム更新、厳重なパスワード要件、定期的なデータバックアップなど、組織がネットワークと情報[28]を安全に保つために行うベストプラクティスの定期的な適用として定義できる。ランサムウェア攻撃を完全に排除することはできないが、適切な予防プロセスを順守することで減らすことができる。また、サイバー犯罪者が使用する実際の攻撃ベクトルは非常に多様で常に変化しているが、適切なサイバー衛生を構成する一連の慣行は比較的確立されており、業界全体で一貫しているため、標準化された評価と長期的な追跡が可能になっている。

サイバーリスクの代用としてサイバー衛生を包括的に評価するために必要な情報は、投資家がより広く利用できるようになっている。従来の ESG データプロバイダーは、発行者のデータプライバシー及び保護ポリシーの主観的な評価を提供する傾向にある。これは重要なテーマだが、このような調査方法では、組織のサイバーセキュリティ・パフォーマンスの正確性または客観性のある全体的な測定値を得ることができない。現在、様々な専門データ提供機関が対象企業に干渉することなく自動化された測定方法に基づいて、サイバー衛生に関する包括的な「サイバーリスク格付」を定期的に更新し、実質的に制限のないほど広い企業カバレッジで提供している。信用リスク格付けが債務不履行の可能性の暗黙の予測により発行者の債務返済能力の予測を反映するのと同様に、サイバーリスク格付は、組織の全体的なサイバーセキュリティ・パフォーマンスと、サイバー侵害またはランサムウェア攻撃の暗黙のリスクを反映するように設計されている。実際、従来型の信用格

[28] Security Scorecard, “What is Cyber Hygiene? Definition, Benefits, & Best Practices,” Mar 2, 2022.

付け会社の中には、サイバーセキュリティリスクの格付けを非財務（ESG）情報の形式として企業の信用格付けに直接組み込むようになったものもある。サイバーセキュリティの情報を発行体リスクの全体的な評価に組み込むことは、投資家にとって経済的に合理的であり、政治的に中立である。サイバーセキュリティのリスクは、企業の信用力の質と投資収益に直接影響を与える可能性があるからである。

３．社債投資における ESG 評価にサイバーセキュリティデータを組み込む NAM のアプローチ

NAM では、社債投資戦略の「ガバナンス」要素として、サイバーセキュリティを独自の ESG 定量評価モデルに直接組み込んでいる。これは、サイバーセキュリティのパフォーマンスが組織の全体的なガバナンス構造を反映しているという当社の見解を反映している。サイバーセキュリティの衛生管理状態が良好であることは、全体的なコーポレートガバナンスが良好であることを示しており、リスクの軽減と質の高い管理の観点から、より魅力的な社債投資であることを示している。当社ではモジュールの組み合わせによる独自の ESG 定量評価モデルの開発に取り組んでおり、サイバーセキュリティなどの新たに出現した重要な課題に対しても、その情報を使用してモデルを柔軟にアップグレードできる。当社の ESG 定量評価モデルのアウトプットは、すべてのグローバル社債の投資戦略におけるスクリーニング、銘柄選択、リスクモニター、発行体エンゲージメントに組み込まれ、サイバーセキュリティリスクのシグナルが債券投資プロセスに体系的に反映されるようにしている。

個々の発行体のサイバーセキュリティのパフォーマンスに加えて、セクター固有のサイバーセキュリティの重要性は、第三者のサイバーリスクデータを全体的な ESG 定量評価モデルに組み込み、企業とのエンゲージメントを優先させるための重要な要素になる。セクター固有のサイバーセキュリティの重要性に関する NAM 独自のマトリックスを作成するために、各業界セクターの相対的なサイバーリスクを次の 3 つの側面に沿って分析する。

１）セクターへのサイバー攻撃による社会経済的影響と損害の可能性
→*重要な商品やサービスの提供に対する潜在的な損害が重大であるほど、サイバーマテリアリティは高くなる。*

２）セクターに対するサイバー攻撃の観測頻度
→*セクターに対するサイバー攻撃の頻度が高いほど、サイバーマテリアリティは高くなる。*

３）セクターにおけるサイバーセキュリティの精巧度と資源の有用性の既存のレベル
→*セクター内の発行体で観測された平均的なサイバーセキュリティ衛生状態が高いほど、サイバーマテリアリティは低くなる。*

このフレームワークに基づき、最も脆弱で、サイバー攻撃者の標的となり、サイバー攻撃による重要なサービス提供への潜在的な損害が大きいセクターに対して、最も高いサイバーマテリアリティを割り当てている。サイバー衛生のパフォーマンスデータは、ESG定量評価モデル全体の入力として、リスク情報に基づき調整することが可能である。

最後に、セクターごとのサイバーセキュリティのマテリアリティを示す「ヒートマップ」は、当社のサイバーセキュリティに関する詳細な調査と投資先企業とのエンゲージメントを行う際の指針として活用される。当社は、個々のパフォーマンスとそのセクターにおけるサイバーマテリアリティの程度に基づき、企業とのサイバーセキュリティ問題へのエンゲージメントを優先する。独自のエンゲージメントのチャネルを通じて特定のサイバーセキュリティの脆弱性に対処することは、当社の投資先企業のサイバーセキュリティのパフォーマンスを体系的に向上させる責任ある効果的な方法であり、財務リスクの軽減と現実世界に影響を与える可能性がある。

VI 結論

企業のサイバーセキュリティは、財務上の重要性（マテリアリティ）が増し、規制や開示環境が急速に変化する中、主流の ESG 投資家が投資の意思決定に組み込む次世代の要素である。企業の客観的かつ比較可能なサイバーセキュリティのパフォーマンスデータは、投資家が投資プロセスの一部として組み込めるようになっている。企業がサイバーセキュリティに十分な注意を払わない「市場の失敗」に対処するために、ESG分析に組み込むことで、企業のサイバーセキュリティのパフォーマンス基準を全面的に高めることができ、社債投資のリスク調整後リターンと社会経済的レジリエンスの向上に貢献する可能性がある。

〔原文 (Original)〕

Integration of Cybersecurity Performance into ESG Analysis and Credit Risk for Sustainable and Resilient Investment

Jason Mortimer,
Head of Sustainable Investment – Fixed Income,
Nomura Asset Management

▌Abstract ▐

1. Cybersecurity for Next Generation ESG Investment Integration and Real-World Impact: ESG investment integration is the consideration of market material, non-financial factors to improve risk-adjusted-returns in a way that also addresses important socio-economic and environmental challenges. The integration of corporate GHG emissions data in investment analysis is one key example of this process. Now Cybersecurity is emerging as a major next-generation ESG factor for mainstream investors, with strong alignment to financial and investment risk, growing regulatory scrutiny, and the potential for real-world impact. In this report, we explore this trend and introduce Nomura Asset Management (NAM)'s approach to integrating Cybersecurity risk in the corporate debt ESG investment process for risk management and corporate engagement.
2. Growing Financial Materiality of Corporate Cybersecurity Risks and Regulatory Response: Investors have a growing interest in assessing the underlying cybersecurity risk inherent in their corporate investment portfolios. Corporate cyber-attacks are growing in severity and frequency as economic digitalization expands the cyber "attack surface" available for hackers to exploit. Inadequate protections in cyberspace also threaten overall economic growth and national security, with global loss estimates from cybercrime reaching 6 trillion USD in 2021. Reflecting this, surveys of global business and political leaders now regularly point to Cybersecurity as a top global risk by impact and likelihood along with climate change and geopolitical conflict. In response, global cybersecurity regulation will increasingly mandate greater corporate cybersecurity performance disclosures with a focus on protection for critical infrastructure and essential services.
3. NAM's approach to integrating Cybersecurity data in Credit ESG analysis: Cybersecurity's growing negative impact and increasing awareness in society is leading investors to integrate this topic into investment research and corporate engagement. Recognizing the investment materiality of cybersecurity, NAM has developed its own proprietary approach for systematically and quantitatively measuring cyber-risk in corporate credit analysis. Using alternative datasets, we analyze the degree to which investee companies practice good "cyber-hygiene" such as regularly patching software vulnerabilities and applying best practices for securing data and networks. Corporate cybersecurity risk and performance data is then directly incorporated as a Governance factor in NAM's proprietary Credit ESG Scoring model for integration in our global fixed income strategies.
4. By raising cybersecurity as an ESG investment topic, NAM hopes to incentivize higher corporate cybersecurity performance standards, contribute to socio-economic resiliency as real world positive impact, and potentially achieve better risk-adjusted credit investment returns for our clients

I Cybersecurity for Next Generation ESG Investment Integration and Real-World Impact

From a practical perspective, ESG integration is the consideration of market material, non-financial factors in investment analysis to improve risk-adjusted-returns in a way that also addresses important socio-economic and environmental challenges. Carbon emissions and climate change are prime examples of how shifts in awareness and market pricing of ESG risks can lead to real-world impact. For example, it is now a mainstream practice for investors to integrate GHG emission disclosures into the investment processes. As a result, trillions of USD of capital are currently being allocated and priced according to investor perceptions of corporate carbon performance. Due to this repricing of corporate risk and valuations, firms have a powerful incentive for emission reductions in support of global climate mitigation efforts. Investors thus achieve real world impact and avoid investment risks by addressing the "market failure" of such previously unpriced negative externalities.

By implication, investors are incentivized to identify new and emerging non-financial ESG factors associated with global challenges with the potential to materially affect market pricing and attract additional regulatory risk. For this, Cybersecurity is emerging as a major next generation ESG consideration for mainstream investors, with strong alignment to financial and investment risk, growing regulatory scrutiny, and the potential for real-world impact.

In this report, we analyze the financial materiality of corporate cybersecurity risk, explore the trend in global regulatory developments, and introduce Nomura Asset Management (NAM)'s approach to integrating Cybersecurity risk in the corporate debt ESG investment process for risk management and corporate engagement.

II Financial Materiality of Corporate Cybersecurity Risk - Micro-Economic (Enterprise) Costs

Investors have a growing interest in assessing the underlying cybersecurity risk inherent in their corporate investment portfolios. Cybercrime affects individual enterprises through increased frequency of data breaches and ransomware attacks, higher corporate cyber defense and insurance spending, and reputational damage. Large-scale cyberattacks can cause operational and business disruption, and generate significant litigation risk.

Cybercrime rates are growing in severity and frequency as economic digitalization expands the cyber "attack surface" available for hackers to exploit. Estimates of the rate of cyber-attacks per company are 31% higher in 2021 compared to 2020[1] with the average cost for individual data breaches in 2022 reaching 4.35 million USD[2]. Ransomware has become a major concern for businesses, with survey data showing that 83% of

1 Accenture, "State of Cybersecurity Resilience 2021," 2021.
2 IBM, "Cost of a Data Breach 2022 Report," July 2022.

organizations experienced a ransomware attack over the past two years. The most commonly demanded ransom amount for US companies is now in the range of 5 to 10 million USD[3].

Corporate cyber defense and insurance spending is emerging as a major cost for businesses. The overall market for business spending on cybersecurity products and services is estimated to reach 1.75 trillion USD for the 5-year period from 2021-2025, compared to 1.0 trillion USD spent from 2017 to 2021[4]. Certain financial firms in the US reportedly spend over 1 billion USD per year just on securing and protecting digital infrastructure and client data, indicating the immense scale of cyber spending in critical sectors. More firms are opting for cyber-insurance, with one US study finding that insurance uptake rates rose from 26% in 2016 to 47% in 2020[5]. Cyber-insurance premiums have risen some 30-40 percent in 2021, and the overall cyber-insurance market is predicted to grow to 34 billion USD by 2031, from approximately 8.5 billion USD in 2021.

Recent major cyberattacks have targeted hospitals and pharmaceutical companies[6], travel and leisure[7] companies, financial services[8], and energy infrastructure[9] operators. Individual events not only disrupt operations and result in hundreds of millions of dollars in business impairment and legal liabilities, they can also compromise sensitive personal data and may threaten national critical functions. In one high profile case in 2017, Chinese military hackers[10] exploited an unpatched software vulnerability to infiltrate a consumer credit reporting agency in the United States. The state-backed cyber-attackers stole personally identifiable information including names, addresses, and Social Security Numbers linked to detailed financial records of approximately 145 million people. When the company disclosed the data breach, its stock declined by a maximum of nearly 35% and credit spreads on its Investment Grade-rated debt widened by 118 basis points. In 2019, the company reached a settlement with the FTC in the US for at least 575 million USD in fines, penalties, and consumer restitution.

III Financial Materiality of Corporate Cybersecurity Risk - Macro-Economic Costs

From a broader society-wide perspective, inadequate protections in cyberspace can lead to macro-economic damages with national strategic implications. These impacts include indirect economic loses from wide scale

3 IBM, ”Cyber Resilient Organization Study 2021,” 2021

4 David Braue, “Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025,” *Cybercrime Magazine*, September 10, 2021.

5 U.S. Government Accountability Office, “Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market,” May 20, 2021.

6 David Voreacos, Katherine Chiglinsky, Riley Griffin, “Merck Cyberattack’s $1.3 Billion Question: Was It an Act of War?,” *Bloomberg*, December 3, 2019.

7 “Marriott Hacking Exposes Data of Up to 500 million Guests,” *The New York Times*, November 30, 2018.

8 Federal Trade Commission, “Equifax Data Breach Settlement,” Sep 2022.

9 “The Colonial Pipeline Hack Is a New Extreme for Ransomware,” *WIRED*, May 8, 2021.

10 Federal Bureau of Investigation, “Chinese Military Hackers Charged in Equifax Breach,” February 10, 2020.

industrial espionage, the erosion of incentives for innovation and investment, and the violation of data privacy. They also include threats to the critical functions and infrastructure that underpin economic and national security, public health, and the safety and freedom of citizens. Investors are increasingly aware that the risks from Cybersecurity are not limited to the companies directly affected but also extend to the entire society that underpins the economy and market valuations.

Economic damages from cybercrime and cyber-espionage are growing at an immense scale. Some sources estimate that global annual losses from cybercrime may reach $10.5 trillion USD *per year* by 2025[11] from $6 trillion USD in 2021. In comparison, a 2021 reinsurance company report[12] estimated economic losses from climate change at $23 trillion *cumulatively* by 2050[13]. While differences in methodology[14] and statistical sampling[15] make it difficult to compare these figures directly, the implication is that the economic impact of cybersecurity may be at a similar scale as global climate change. Reflecting this, Cybersecurity consistently ranks in the top 5 global risks in perception surveys of global CEOs[16] and decision-makers[17] together with climate change and geopolitical conflict.

The sectors most often targeted by cyberattacks are Finance, Healthcare, Information Technology, and Manufacturing[18], with a particular increase in cybercrime targeting the health and pharmaceutical sector during the Covid pandemic. In addition to providing high value monetary targets for financially-motivated cyber criminals, these sectors are also associated with Critical National Functions where disruption or destruction would have high strategic value to state-backed cyber attackers. These sectors also tend to have a high degree of non-tangible intellectual property that is an attractive target for hackers with both financial and geopolitical motivations. In 2013, a senior official in the US National Security Agency (NSA) described cyber-espionage as "the greatest transfer of wealth in history[19]".

Market participants are increasingly aware of the growing direct and indirect costs from weak corporate cybersecurity. Based on this trend, more investors are now beginning to incorporate cybersecurity performance as a non-financial (ESG) factor for analysis in corporate investment.

---

11 "2022 Cybersecurity Almanac," *Cybercrime Magazine*, January 19, 2022.
12 Swiss Re Group, "Climate Action – This is a Mission Possible," November 3, 2021.
13 "Climate Change Could Cut World Economy by $23 Trillion in 2050, Insurance Giant Warns," *The New York Times*, April 22, 2021.
14 Organisation for Economic Co-operation and Development, "Losses and Damages from Climate Change."
15 Dinei Florencio and Cormac Herley, "Sex, Lies and Cyber-crime Surveys," *Microsoft Research*, June 2011.
16 PWC, "PwC 25th Annual Global CEO Survey Reimagining the Outcomes that Matter," January 17, 2022.
17 World Economic Forum, "These are the Biggest Global Risks," January 16, 2019.
18 Statista, "Global Industry Sectors Most Targeted by Basic Web Application Attacks from November 2020 to October 2021," May 2022.
19 Infosec, "Cyber-Espionage: The Greatest Transfer of Wealth in History," February 12, 2013.

IV Overview of Recent Cybersecurity Global Regulatory Developments

Corporate investors face a rapidly changing regulatory environment for cybersecurity. Cybersecurity's growing costs to society amid rising geopolitical competition make it a growing topic of focus for global policy makers, with 80% of governments around the world having now enacted cybercrime legislation and data protection legislation[20]. Updates and additions to cybersecurity legislation are progressing in the USA, European Union (EU), UK and Japan, with a trend for greater regulatory oversight, disclosure requirements, and coverage for critical infrastructure and essential services.

1. USA

The US Federal Trade Commission, Securities and Exchange Commission, and Cybersecurity and Infrastructure Security Agency have all proposed new regulations at the national level in 2022. The emerging focus of cybersecurity regulation in the US is focused on cyber breach reporting, supply chain cybersecurity compliance, and possible legal liability for firms that fail to patch known software vulnerabilities leading to the loss of consumer data. In the first half of 2022, 24 US states have enacted new cybersecurity legislation[21], mostly focused on setting cybersecurity standards and increasing funding for cybersecurity programs in the public sector, cybersecurity general workforce training, and enhancing the integrity of election and voting systems.

2. EU

In the EU, major cyber-related regulation has focused on consumer protection. The landmark European General Data Protection regulation (GDPR) came into force in 2016, dealing with the handling and management of personal data and online privacy. In 2022, the European Cyber Resilience Act[22] has been proposed to mandate cybersecurity requirements for hardware and software products sold in the EU throughout the product's lifetime. The EU has also recently passed an updated Network and Information Systems Directive[23] (NIS 2 Directive) as a package of measure to improve the resilience and incident response capabilities in the EU, with an emphasis on critical infrastructure protection and updated incident management and reporting obligations[24].

[20] United Nations Conference on Trade and Development, "Global Cyberlaw Tracker." <https://unctad.org/page/cyberlaw-tracker-country-detail, accessed on October 10, 2022>

[21] National Conference of State Legislatures, "Cybersecurity Legislation 2021," July 1, 2022.

[22] European Commission, "Cyber Resilience Act – Factsheet," September 15, 2022.

[23] European Commission, "NIS Directive." <https://digital-strategy.ec.europa.eu/en/policies/nis-directive, accessed on June 7, 2022>

[24] European Council, "Strengthening EU-wide cybersecurity and resilience – provisional agreement by the Council and the European Parliament," May 13, 2022.

3. United Kingdom

The post-Brexit UK-GDPR has been retained with the same key principles and rights, and obligations as the original EU version[25]. The Security of Network & Information Systems Regulations (NIS Regulations) passed in 2018 is a legal measure to enhance the cyber resilience of information networks and critical national infrastructure for essential services. The UK government is currently evaluating options for incentivizing private industry to make greater investments in cyber security. Initial government reports on this topic have recognized that market incentives and more interventionist regulations may be needed to more quickly establish better practices in the changing risk environment[26].

4. Japan

Japan's cybersecurity regulation and legislation is seen as relatively less advanced than other developed countries. The Basic Act on Cybersecurity represents Japan's fundamental law on cybersecurity, while the Act on the Protection of Personal Information (APPI) is the country's main legislation for data protection. Amendments to the APPI in 2022 mandate reporting and notification in the case of personal data breaches, but there are so far no obligations for cyber breach reporting in other cases. Japan also currently lacks specific regulations for secure software development. Reflecting trends in the US, EU, and UK, the Japanese government is now considering the introduction of an Active Cyber Defense (ACD) framework covering critical infrastructure that would authorize government access to network systems for monitoring and analyzing suspicious communications.[27]

V NAM's approach to Cybersecurity in Credit Analysis and Engagement

The growing negative impact and rising risks for companies and society, increased public awareness of cybersecurity risks and their negative effects, and rising political scrutiny with stricter regulation are all factors pushing the widespread adoption of cybersecurity for investment managers. Recognizing the growing materiality of cybersecurity to investors, NAM developed its own proprietary approach to systematically and quantitatively integrating cybersecurity into credit analysis.

1. Understanding Cybersecurity risk as a "Market Failure"

As the first step of NAM's cybersecurity integration buildout, we considered the current challenges faced by the market for effectively recognizing, assessing, and pricing corporate cybersecurity risks.

First, corporate cybersecurity has traditionally been treated as an extension of the IT department. This tendency has led many corporates to view cybersecurity preparedness and resiliency as a compliance cost to

[25] Information Commissioner's Office, "The UK GDPR."
[26] Government Digital Service, "2022 cyber security incentives and regulation review," January 19, 2022.
[27] "Active Cyber Defense Framework could One Day Protect Japan," *The Japan News*, September 13, 2022.

be minimized rather than as a source of operational excellence. As a result, spending on cybersecurity preparedness is often insufficient relative to the level of risk. Corporate cybersecurity reporting lines and responsibilities are often unclear, and board oversight and expertise in this topic is limited. Insufficient prioritization of corporate cybersecurity has contributed to the shortfall of expertise and human resources seen today. Therefore it is important to raise the status of cybersecurity among investors and corporate managers to a more strategic operational and business level, to commit the necessary level of investment and develop a sufficient pipeline of cybersecurity professionals to meet the market need.

Second, cybersecurity has generally existed outside the purview of legislation and regulation. Most digital infrastructure is privately owned, so cybersecurity policies are typically based on “best practices” rather than regulatory requirements. This has left cybersecurity implementation as an internal corporate function without sufficient oversight from government or investors. Most cyber incidents and breaches are not publically reported or acknowledged, making it difficult for investors to assess cybersecurity risks. To some degree, this situation is understandable, since corporations want to avoid embarrassment and potentially additional costs from disclosing cyber incidents, especially when there is no legal requirement to do so. Going forward, the systematic integration of cybersecurity risks in investment analysis will create demand for more material cybersecurity-related disclosures. At the same time updates to cybersecurity regulatory will require more disclosure of breach and mandate greater cybersecurity preparedness especially in critical infrastructure and essential services.

Third, there is no “one-size-fits-all” approach to effectively addressing corporate cybersecurity risk. It is not easy to standardize the evaluation of cybersecurity performance across companies. Cybercriminals opportunistically target areas of weakness with a variety of intrusion strategies, so risk vectors and attack methods are constantly changing. This means that cybersecurity defenders cannot just focus on a specific set of high-risk systems or processes, or rely on any single method of prevention. By extension, investors cannot use a generalized framework for assessing the idiosyncratic cybersecurity risks between companies based on comparative evaluations of known weak points. And as with any form of crime, cybercrime is difficult if not impossible to predict. Firms do not usually disclose meaningful details about their cybersecurity policies and performance to public investors, and there are legitimate concerns that too much disclosure of cyber vulnerabilities would only attract more cyber-attacks. Together this implies that investors evaluating cybersecurity across companies will have to rely on ex-ante measures of cybersecurity preparedness and adherence to best practices as a proxy for cybersecurity risk.

These challenges have made it difficult for investors to comprehensively integrate cybersecurity risks in the investment process. In particular, the lack of comparable cybersecurity performance data or methods for measuring it have prevented markets from efficiently pricing corporate cybersecurity risks. With a lack of market pressure and so-far limited regulatory requirements, corporates tend to underinvest in their own

cybersecurity and thus are more likely to suffer cyberattacks than would otherwise be the case. But the harm from this underinvestment in cybersecurity protection also extends to customers, citizens, and society at large. In other words, systematic underpricing of cybersecurity risk represents a market failure, similar to the negative externalities caused by carbon emissions and industrial pollution and waste.

2. How NAM has adopted Cybersecurity data as a next generation ESG factor

To effectively and comprehensively address the challenges of assessing and integrating cybersecurity risk in corporate debt investments, at NAM we focus on systematic measurement of "cybersecurity hygiene". Cyber hygiene can be defined as the regular application of best practices that an organization takes to keep its network and data secure[28], such as regular patching of known vulnerabilities, strong password requirements, and regular data backups, etc. While the risk of a data breach or ransomware attack can never be completely eliminated, it can be reduced by adherence to good cyber hygiene. And while the actual attack vectors used by cybercriminals are highly diverse and constantly changing, the set of practices that constitutes good cyber hygiene are relatively established and consistent across industries, allowing for standardized evaluations and tracking over time.

The data required for comprehensively evaluating cybersecurity hygiene as a proxy for cyber risk is becoming more widely available to investors. Traditional ESG data providers tend to provide subjective assessments of issuers data privacy and protection policies. This is an important topic, but such survey methods cannot give an accurate or objective overall measure of organizational cybersecurity performance. A variety of specialized data providers now provide comprehensive "cyber risk ratings" based on automated, non-intrusive measurements of cyber hygiene with regular updates and effectively unlimited issuer coverage. Just as credit risk ratings reflect the issuer's predicted ability to pay back debt with an implicit forecast of the likelihood of default, cyber risk ratings are designed to reflect the organization's overall cybersecurity performance and implied risk of cyber breach or ransomware attack. In fact, some traditional credit ratings firms now integrate cybersecurity risk ratings directly into their corporate credit ratings as a form of non-financial (ESG) data. Integrating cybersecurity data into the overall evaluation of issuer risk is economically rational and politically neutral for investors, because cybersecurity risks can have a direct impact on credit quality and investment returns.

3. NAM's approach to integrating Cybersecurity data in Credit ESG analysis

At NAM, we integrate Cybersecurity directly into our proprietary Credit ESG Scoring model as a "Governance" factor for corporate debt investment strategies. This reflects our view that cybersecurity performance is a reflection of an organization's overall governance structure. Good cybersecurity hygiene is indicative of overall good corporate governance, and a more attractive corporate debt investment from the

[28] Security Scorecard, "What is Cyber Hygiene? Definition, Benefits, & Best Practices," March 2, 2022.

perspective of risk-reduction and high quality management. Since NAM has developed a proprietary Credit ESG Scoring system that is modular and flexible, we can upgrade our model over time with data for newly emerging material issues such as cybersecurity. The NAM Credit ESG Score model outputs are integrated into screening, security selection, risk monitoring, and issuer engagement across all global corporate credit strategies, ensuring that cybersecurity risk signals are systemically reflected in our fixed income investment process.

In addition to the cybersecurity performance of individual issuers, sector-specific cybersecurity materiality is a crucial element for integrating third party cyber risk data into the overall credit ESG model and for prioritizing engagement with companies. To generate NAM's proprietary matrix of sector-specific cybersecurity materiality, we analyze the relative cyber risk for each industry sector along three dimensions:

1) The potential for socio-economic impact and damage from cyber-attacks on the sector
   → *The more critical the potential damage to the provision of essential goods and services, the higher the cyber materiality*

2) The observed frequency of cyberattacks against the sector
   → *The higher the frequency of cyberattacks against the sector, the higher the cyber materiality*

3) The existing level of cybersecurity sophistication and resource availability in the sector
   → *The higher the observed average cybersecurity hygiene for issuers in the sector, the lower the cyber materiality*

Based on this framework, we assign the highest cyber materiality to sectors that are the most vulnerable and most frequently targeted by cyber attackers, and where the damage from cyber-attacks on the provision of essential services is potentially the greatest. Cyber hygiene performance data can then be adjusted on a risk-informed basis as an input for the overall credit ESG scoring model.

Finally, the resulting "heat map" of sector-specific cybersecurity materiality acts as a guide for our in-depth corporate cybersecurity research and engagement with investee companies. We prioritize engagement on cybersecurity issues with companies based on their individual performance and the degree of cyber materiality in their sector. Addressing specific cybersecurity vulnerabilities through private engagement channels is a responsible and effective way of systematically raising the cyber security performance of our portfolio companies, potentially resulting in financial risk reduction and real-world impact.

VI Conclusion

With growing financial materiality and a rapidly changing regulatory and disclosure environment, corporate cybersecurity is a next generation factor for mainstream ESG investors to integrate into investment decision making. Objective and comparable cybersecurity performance data for corporates is increasingly available for investors to integrate as part of the investment process. Addressing the “market failure” of insufficient attention to corporate cybersecurity by incorporating it into ESG analysis can incentivize higher corporate cybersecurity performance standards across the board, potentially contributing to better risk-adjusted-returns and socio-economic resiliency as real world positive impact.