Bond Blog

September 26, 2023

PGIM FIXED INCOME

Cybersecurity: How it Affects ESG Impact and Credit Quality

Birgit Lundem Jakobsen, Senior ESG Analyst

Cyberattacks are becoming more frequent and more damaging. To prevent negative ESG impact and credit deterioration from such attacks, companies need to keep up with rapid technological developments.

Industry-level considerations can indicate which sectors are most at risk of cyberattacks. But company-level analysis is crucial, and that's more nuanced work. Best practice for companies includes thorough cyber-hygiene, strong governance, and board-level expertise.

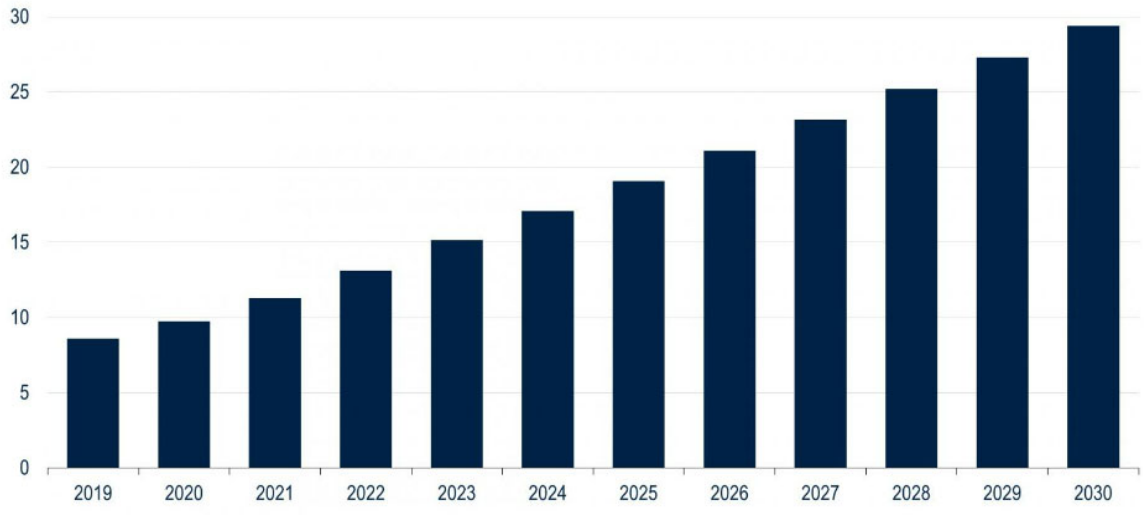
With the right analysis, investors can gauge which firms apply basic, better, or best practice. Such an assessment can put cybersecurity on the corporate agenda and protect clients' assets.

An Ever More Connected World Is Increasingly Vulnerable to Cyberattacks

Digitalization, cloud computing, artificial intelligence (AI), and billions of connected devices are increasingly leaving companies vulnerable to cybercrime.

In 2019, the Internet of Things consisted of 8.6 billion connected devices worldwide, versus almost none a decade earlier. In the four years since 2019, that number has almost doubled, to 15.14 billion, nearly twice the global population. And the number of IoT-connected devices is expected to almost double again, to 29.4 billion, by 2030 (see Figure 1).[1]

FIGURE 1: Number of Internet-connected devices worldwide (billions)



Source: Transforma Insights.

The rising volume of connected devices has led to an exponential surge in cybercrime, but preparedness remains low. In a 2022 IBM survey, 83% of companies had experienced more than one cyberattack in the past year.[2] However, a 2020 survey by McAfee and CICS showed that only 44% of respondents had plans in place to prevent and respond to IT security incidents.[3]

Most Cyberattacks Are Financially Material

Not all companies understand how quickly cybercrime is growing. And many firms underappreciate the strategic risk it presents, or the strategic opportunities that strong cybersecurity may bring, e.g., as a competitive advantage.

This lack of understanding of and investment in cybersecurity can be financially material. In our view, cybersecurity considerations are important in analyzing both ESG risk and ESG impact. (More information in Figure 3 below, and at ESG Investing at PGIM Fixed Income.)

Well-known financial implications of cyber-incidents include direct costs such as breach response, litigation, regulatory compliance, and cybersecurity improvements. But in most cases, the financial impact of a data breach ranges much wider. It can include operational disruption, devaluation of trade name, loss of customers, credit deterioration, and, ultimately, increased capital markets costs.

These wider impacts are often less public, less quantifiable, and longer-term. But often, they make up a large (sometimes: the largest) part of total losses incurred.

For example, multinational consumer credit agency Equifax was subject to a data breach in 2017, which compromised private records of more than 160 million users. Prior to the breach, the company issued 10-year U.S.-dollar denominated debt at 150 basis points (bps) over U.S. Treasury yields. In 2019, credit rating agency S&P downgraded Equifax's rating from BBB+ to BBB, stating "we expect Equifax's leverage will remain elevated over the next 18 months, kept aloft by substantial investments in network, data, and application security architecture; in modernizing technology and business platforms; in new product development; and in remedying the reputational damage from the breach."[4] In 2020, the company issues 10-year U.S.-dollar debt at 250 bps over U.S. Treasuries.

Good Governance Includes Strong Cybersecurity

From an ESG impact perspective, companies have a responsibility to maintain strong cybersecurity. Not only is sensitive customer data at risk, but a compromised IT system can also endanger critical equipment. Both threats can cause significant social and environmental damage, including the exposure of sensitive personal data, identity theft, catastrophic spills, shutdowns of critical infrastructure, and manipulation of social media.

The NotPetya ransomware attack in 2017 was one of the largest cyberattacks in history. It shut down Ukraine’s electrical grid and resulted in financial losses estimated at $10 billion.

Even smaller cyber incidents, however, can bring about severe consequences. In February 2021, a hacker gained access to a water treatment plant in Florida. In a matter of minutes, the hacker increased the level of sodium hydroxide 100 times. This attack could have poisoned the local population, had the plant’s operator not detected and immediately remedied it.

Other cyberattacks have proved fatal. A 2020 ransomware attack forced a hospital in Germany to close its emergency department. A patient due to undergo treatment was rerouted to another hospital but died en route, the first death directly attributed to ransomware. A 2021 study by Californian cybersecurity firm Proofpoint and the Ponemon Institute in Michigan surveyed more than 600 healthcare facilities. Their study found that ransomware attacks increased mortality rates at a quarter of the facilities surveyed.[5]

Which Industries Are Most Vulnerable?

Today, all companies are inevitably exposed to cyber risk. But the extent of that risk depends on several circumstances. In our view, sector characteristics and cyber-preparedness are key investor considerations.

Industries such as manufacturing, finance and insurance, as well as professional, business and consumer services, are the most heavily targeted, according to IBM.[6] Manufacturing firms have low tolerance to disruption, especially since the supply chain pressures after the pandemic. In financial firms, compromised systems can put world trade on hold, and the industry holds sensitive information on its clients. Professional, business, and consumer services firms hold sensitive personal data as well. All three sectors are targets because they have the capacity to comply with financial demands.

FIGURE 2: Share of cyberattacks by industry

Industry	2022	2021	2020	2019	2018
Manufacturing	24.8	23.2	17.7	8	10
Finance and insurance	18.9	22.4	23	17	19
Professional, business and consumer services	14.6	12.7	8.7	10	12
Energy	10.7	8.2	11.1	6	6
Retail and wholesale	8.7	7.3	10.2	16	11
Education	7.3	2.8	4	8	6
Healthcare	5.8	5.1	6.6	3	6
Government	4.8	2.8	7.9	8	8
Transportation	3.9	4	5.1	13	13
Media and telecom	0.5	2.5	5.7	10	8

Source: IBM X-Force Threat Intelligence Index 2023

In other published data, government, financial, business, and professional companies, and the healthcare sector feature as the most targeted industries. Where the motivation is ransom, manufacturing and retail/wholesale also feature prominently.

All in all, a hacker's perspective is arguably influenced by:

- the impact that a cyberattack can have in terms of business disruption, internal and external to the company targeted. For example, critical infrastructure - including manufacturing, utilities, healthcare, and banks - is highly attractive. Companies in this industry generally don't tolerate downtime, because it is costly and because any disruption can severely impact stakeholders;
- the extent and sensitivity of data that the company holds. Sensitive information can be wide-ranging, from corporate to personal data. Industries where sensitive personal information is particularly prevalent include government agencies, financial firms, and healthcare institutions; and/or
- a company's ability to comply with financial demands in a ransomware attack.

A 2021 ransomware attack on Colonial Pipeline, a major U.S. fuel pipeline operator, is a good example of an attack on critical infrastructure that had major impacts outside of the company. Hackers entered Colonial's IT systems, infecting it with ransomware and stealing data. To prevent the ransomware from spreading, Colonial shut down its pipeline for days.

The pipeline carried 45% of the gas, diesel, and jet fuel supplied to the U.S. East Coast, so its shutdown led to widespread fuel shortages and prompted an "All-of-Government" response.[7]

The 2017 Equifax hack mentioned earlier is a good example of a cyberattack that exposed sensitive personal information. More recently, in 2021, mobile telecoms operator T-Mobile suffered a 2021 cyberattack that compromised the personal information of roughly 76 million people. According to a class action lawsuit that followed, the compromised information included combinations of consumers' names, addresses, phone numbers, dates of birth, Social Security or tax identification numbers, other government ID numbers, account information, mobile phone identifier numbers, PINs, and personal unlock codes.[8]

T-Mobile settled with the claimants for $350 million and committed to invest $150 million in data security and cybersecurity technology. But in November 2022, the company suffered another cyberattack involving data theft, including addresses, phone numbers, and dates of birth of 37 million customers.

How Can Investors Assess An Individual Company's Cyber-Preparedness?

Industry characteristics are a good first step to assess how attractive a company is to hackers. But the more nuanced, and more important, part of that assessment is looking at individual companies themselves. That assessment can be difficult, given companies' sensitivities around disclosing information on cyber-precautions.

Gaining an understanding of a company's cyber-preparedness by analyzing company information provides is a good starting point. An assessment of cyber-preparedness should not only include which security software that has been installed, but should also include considerations around governance, management of cyber risk, the structure around cybersecurity, incident responses, and processes for defense and containment. Figure 3 shows how we think about cybersecurity at the issuer level.

FIGURE 3: Evaluating a bond issuers' cybersecurity

Base line	Better Practice	Best practice
• Solid cybersecurity management and organization, with good cybersecurity technology. • "Base line" companies are likely to consider cybersecurity a compliance issue, as opposed to a strategic risk/opportunity. They may treat some or all of their policies as more check- box exercises. • Ultimate responsibility for cybersecurity lies with the company's board of directors. • Has cyber insurance.	• Strong governance, with board-level responsibility and expertise. The board of directors and C-suite is able to articulate the threat of cyber risk and the company's strategy. • Proper governance, risk management, and compliance processes are in place, with sufficient budget support, including employee training. • Governance fully incorporates considerations around cyber risk related to suppliers and events (such as the cybersecurity of IT integration after an M&A transaction).	• Board and management understand that cybersecurity is both a strategic risk and a strategic opportunity. • Best practice includes regular testing of cyber defenses including "red team" exercises or dummy attacks, employee stress-testing. and recovery plans.

Source: PGIM Fixed Income.

Engaging with companies on the topic is likely to give investors an even better view of what management knows and its level of involvement. Are they able to elaborate on cybersecurity and what it means for their company? Are reporting lines and incident plans in place? What is the level of historical incidents, how were past incidents handled and what did the company learn from the experience?

All these and more questions to management can offer a more nuanced understanding of a company's preparedness.

For information on PGIM Fixed Income's general approach to ESG Engagements, visit the ESG Engagement page.

Other considerations

Cyber security is ever evolving, so companies and investors are wise to constantly consider new developments.

Customers have increased their focus on privacy and data security, and regulators are taking notice. On 26 July 2023 the U.S. Securities and Exchange Commission (SEC) announced new rules that will come into force in December 2023. These rules require publicly listed firms to disclose serious incidents within four days and to annually disclose material information regarding their cyber risk management, strategy, and governance.[9] Across the pond, the EU is strengthening its EU Cybersecurity Act.

In Ireland, Meta was fined €1.2 billion in May 2023 for transferring user data between Europe and the U.S. No actual breach occurred, but Ireland's Data Protection Commission considered that Meta had violated the EU's General Data Protection Regulation (GDPR). In the U.S., attention to consumer privacy has increased as well. In July 2023, the Biden administration announced a cybersecurity labeling program for smart devices to protect American consumers.[10]

Cyber insurance is another sector that continues to evolve. The cost of cyber insurance has doubled, on average, in each of the past three years. And some insurance companies no longer provide cover against state-backed cyberattacks.[11] Such exclusions are likely to worry all industries, particularly utilities and banks, which are prime targets.

Finally, AI and quantum computing are likely to dramatically change cybersecurity. Both can strengthen cybersecurity through more robust encryption algorithms, but attackers are also likely to use them. AI cybercrime tools already enhance and automate phishing attacks and generate malicious codes. Quantum computing would have the capacity to nullify much of today's encryption technologies and comprise the data they protect. Indeed, cybercriminals are already harvesting encrypted data that they currently cannot access, waiting to get their hands on quantum computing to decrypt it.

Conclusion

In a rapidly expanding digital world, cyberattacks are becoming more frequent and more harmful. Their implications, in terms of ESG impact and credit quality, can be significant and material: cyberattacks can result in acute, short-term financial costs as well as long-term impacts on companies and their stakeholders.

For the above reasons, companies need to stay abreast of rapid technological developments. Best practice includes thorough cyber-hygiene, strong governance, and board-level expertise. With the right analysis, investors like us can help protect clients' assets and put cybersecurity on the corporate agenda. That goal should form part of every investor's credit and ESG assessment.

1. Transforma Insights. "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030." July 2023.

2. "Cost of a Data Breach Report 2023. IBM.

3. Gann, Tom. "The Hidden Costs of Cybercrime on Government." McAfee, Dec 21, 2020.

4. "Equifax Inc. Downgraded To 'BBB' On Rising Leverage." S&P Global Ratings, 15 Mar 2020.

5. Miller, Maggie. "The mounting death toll of hospital cyberattacks." Politico, 12/28/2022.

6. "X-Force Threat Intelligence Index 2023." IBM Security. The report provides essential findings based on threat data and responses to incidents with which IBM has been involved.

7. "FACT SHEET: The Biden-Harris Administration Has Launched an All-of-Government Effort to Address Colonial Pipeline Incident." The White House, May 11, 2021.

8. "T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack." August 17, 2021.

9. "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure by Public Companies." U.S. Securities and Exchange Commission, July 26, 2023.

10. "Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers." The White House, July 18, 2023.

11. Patten, Sally. "Cyber insurance premiums soar 80pc as claims surge." Financial Review, Sep 12, 2022.

Important Information

PGIM Fixed Income operates primarily through PGIM, Inc., a registered investment adviser under the U.S. Investment Advisers Act of 1940, as amended, and a Prudential Financial, Inc. ("PFI") company. Registration as a registered investment adviser does not imply a certain level or skill or training. PGIM Fixed Income is headquartered in Newark, New Jersey and also includes the following businesses globally: (i) the public fixed income unit within PGIM Limited, located in London; (ii) PGIM Netherlands B.V., located in Amsterdam; (iii) PGIM Japan Co., Ltd. ("PGIM Japan"), located in Tokyo; (iv) the public fixed income unit within PGIM (Hong Kong) Ltd. located in Hong Kong; and (v) the public fixed income unit within PGIM (Singapore) Pte. Ltd., located in Singapore ("PGIM Singapore"). PFI of the United States is not affiliated in any manner with Prudential plc, incorporated in the United Kingdom or with Prudential Assurance Company, a subsidiary of M&G plc, incorporated in the United Kingdom. Prudential, PGIM, their respective logos, and the Rock symbol are service marks of PFI and its related entities, registered in many jurisdictions worldwide.

These materials are for informational or educational purposes only. The information is not intended as investment advice and is not a recommendation about managing or investing assets. In providing these materials, PGIM is not acting as your fiduciary. PGIM Fixed Income as a general matter provides services to qualified institutions, financial intermediaries and institutional investors. Investors seeking information regarding their particular investment needs should contact their own financial professional.

These materials represent the views and opinions of the author(s) regarding the economic conditions, asset classes, securities, issuers or financial instruments referenced herein. Distribution of this information to any person other than the person to whom it was originally delivered and to such person's advisers is unauthorized, and any reproduction of these materials, in whole or in part, or the divulgence of any of the contents hereof, without prior consent of PGIM Fixed Income is prohibited. Certain information contained herein has been obtained from sources that PGIM Fixed Income believes to be reliable as of the date presented; however, PGIM Fixed Income cannot guarantee the accuracy of such information, assure its completeness, or warrant such information will not be changed. The information contained herein is current as of the date of issuance (or such earlier date as referenced herein) and is subject to change without notice. PGIM Fixed Income has no obligation to update any or all of such information; nor do we make any express or implied warranties or representations as to the completeness or accuracy.

Any forecasts, estimates and certain information contained herein are based upon proprietary research and should not be interpreted as investment advice, as an offer or solicitation, nor as the purchase or sale of any financial instrument. Forecasts and estimates have certain inherent limitations, and unlike an actual performance record, do not reflect actual trading, liquidity constraints, fee. These materials are not intended as an offer or solicitation with respect to the purchase or sale of any security or other financial instrument or any investment management services and should not be used as the basis for any investment decision. PGIM Fixed Income and its affiliates may make investment decisions that are inconsistent with the recommendations or views expressed herein, including for proprietary accounts of PGIM Fixed Income or its affiliates.

Investing in the bond market is subject to risks, including market, interest rate, issuer, credit, inflation risk, and liquidity risk. The value of most bonds and bond strategies are impacted by changes in interest rates. Bonds and bond strategies with longer durations tend to be more sensitive and volatile than those with shorter durations; bond prices generally fall as interest rates rise, and low interest rate environments increase this risk. Reductions in bond counterparty capacity may contribute to decreased market liquidity and increased price volatility. Bond investments may be worth more or less than the original cost when redeemed. Mortgage- and asset-backed securities may be sensitive to changes in interest rates, subject to early repayment risk, and while generally supported by a government, government agency or private guarantor, there is no assurance that the guarantor will meet its obligations. High yield, lower-rated securities involve greater risk than higher-rated securities; portfolios that invest in them may be subject to greater levels of credit and liquidity risk than portfolios that do not. Investing in foreign-denominated and/or -domiciled securities may involve heightened risk due to currency fluctuations, and economic and political risks, which may be enhanced in emerging markets. Currency rates may fluctuate significantly over short periods of time and may reduce the returns of a portfolio. Commodities contain heightened risk, including market, political, regulatory and natural conditions, and may not be suitable for all investors. Diversification does not ensure against loss.

In the United Kingdom, information is issued by PGIM Limited with registered office: Grand Buildings, 1-3 Strand, Trafalgar Square, London, WC2N 5HR. PGIM Limited is authorised and regulated by the Financial Conduct Authority ("FCA") of the United Kingdom (Firm Reference Number 193418). In the European Economic Area ("EEA"), information is issued by PGIM Netherlands B.V., an entity authorised by the Autoriteit Financiële Markten ("AFM") in the Netherlands and operating on the basis of a European passport. In certain EEA countries, information is, where permitted, presented by PGIM Limited in reliance of provisions, exemptions or licenses available to PGIM Limited under temporary permission arrangements following the exit of the United Kingdom from the European Union. These materials are issued by PGIM Limited and/or PGIM Netherlands B.V. to persons who are professional clients as defined under the rules of the FCA and/or to persons who are professional clients as defined in the relevant local implementation of Directive 2014/65/EU (MiFID II). In certain countries in Asia-Pacific, information is presented by PGIM (Singapore) Pte. Ltd., a Singapore investment manager registered with and licensed by the Monetary Authority of Singapore. In Japan, information is presented by PGIM Japan Co. Ltd., registered investment adviser with the Japanese Financial Services Agency. In South Korea, information is presented by PGIM, Inc., which is licensed to provide discretionary investment management services directly to South Korean investors. In Hong Kong, information is provided by PGIM (Hong Kong) Limited, a regulated entity with the Securities & Futures Commission in Hong Kong to professional investors as defined in Section 1 of Part 1 of Schedule 1 (paragraph (a) to (i) of the Securities and Futures Ordinance (Cap.571). In Australia, this information is presented by PGIM (Australia) Pty Ltd ("PGIM Australia") for the general information of its "wholesale" customers (as defined in the Corporations Act 2001). PGIM Australia is a representative of PGIM Limited, which is exempt from the requirement to hold an Australian Financial Services License under the Australian Corporations Act 2001 in respect of financial services. PGIM Limited is exempt by virtue of its regulation by the FCA (Reg: 193418) under the laws of the United Kingdom and the application of ASIC Class Order 03/1099. The laws of the United Kingdom differ from Australian laws. In Canada, pursuant to the international adviser registration exemption in National Instrument 31-103, PGIM, Inc. is informing you that: (1) PGIM, Inc. is not registered in Canada and is advising you in reliance upon an exemption from the adviser registration requirement under National Instrument 31-103; (2) PGIM, Inc.'s jurisdiction of residence is New Jersey, U.S.A.; (3) there may be difficulty enforcing legal rights against PGIM, Inc. because it is resident outside of Canada and all or substantially all of its assets may be situated outside of Canada; and (4) the name and address of the agent for service of process of PGIM, Inc. in the applicable Provinces of Canada are as follows: in Québec: Borden Ladner Gervais LLP, 1000 de La Gauchetière Street West, Suite 900 Montréal, QC H3B 5H4; in British Columbia: Borden Ladner Gervais LLP, 1200 Waterfront Centre, 200 Burrard Street, Vancouver, BC V7X 1T2; in Ontario: Borden Ladner Gervais LLP, 22 Adelaide Street West, Suite 3400, Toronto, ON M5H 4E3; in Nova Scotia: Cox & Palmer, Q.C., 1100 Purdy's Wharf Tower One, 1959 Upper Water Street, P.O. Box 2380 - Stn Central RPO, Halifax, NS B3J 3E5; in Alberta: Borden Ladner Gervais LLP, 530 Third Avenue S.W., Calgary, AB T2P R3.

留意事項

※本資料はPGIMフィクト・インカムが市場動向に関する情報提供としてプロの投資家向けに作成したものです。PGIMフィクスト・インカムは、米国SECの登録投資顧問会社であるPGIMインクの債券運用部門です。

※本資料は情報提供を目的としたものであり、特定の金融商品の勧誘又は販売を目的としたものではありません。また、本資料に記載された内容等については今後変更されることもあります。

※記載されている市場動向等は現時点での見解であり、これらは今後変更することもあります。また、その結果の確実性を表明するものではなく、将来の市場環境の変動等を保証するものでもありません。

※本資料で言及されている個別銘柄は例示のみを目的とするものであり、特定の個別銘柄への投資を推奨するものではありません。

※本資料に記載されている市場関連データ及び情報等は信頼できると判断した各種情報源から入手したものですが、その情報の正確性、確実性について当社が保証するものではありません。

※本資料に掲載された各インデックスに関する知的財産権及びその他の一切の権利は、各インデックスの開発、算出、公表を行う各社に帰属します。

※過去の運用実績は必ずしも将来の運用成果等を保証するものではありません。

※本資料は法務、会計、税務上のアドバイスあるいは投資推奨等を行うために作成されたものではありません。

※PGIMジャパン株式会社は、世界最大級の金融サービス機関プルデンシャル・ファイナンシャルの一員であり、英国プルーデンシャル社とはなんら関係がありません。

PGIMジャパン株式会社
金融商品取引業者 関東財務局長（金商）第392号
加入協会：一般社団法人日本投資顧問業協会、 一般社団法人投資信託協会、一般社団法人第二種金融商品取引業協会
PGIMJ102186