

# Sustainability Now Podcast

## “Cyberattack in Aisle Three”

Transcript, 30 January 2026

Speaker 1: Hello and welcome to the weekly edition of Sustainability Now, the show where we explore how the environment, our society and corporate governance affects and are affected by our economy. I am Gabriela de la Serna, and I am your host for today's episode.

I'm based in London and here just like in most places around the world, the experience of supermarket shopping has become pretty seamless. Now in 2026, I can walk into my local store, pick up a few snacks, tap my card at the till, and be on my way in minutes. It feels very seamless, until it isn't.

And last year, a series of cyber attacks on UK retailers showed just how fragile the network of data and logistics behind that seamless experience really is. The disruption was serious, serious enough that the UK government is now treating these kinds of attacks as a national security issue. And to try to reduce the impact of future attacks, it has even proposed to limit a company's ability to pay ransoms to hackers.

So on today's episode, we are unpacking why cyber attacks are becoming an emerging risk for food retailers, how prepared companies really are, and why investors should be paying close attention. So, let's jump right in.

Over the past year, here in the UK, we've seen what happens when that digital infrastructure is disrupted. Some of the country's best known retailers, including Marks & Spencer's and Co-op, have been hit by cyber attacks that forced parts of their operations offline.

And in the case of M&S, the impact of the attack went well beyond a short-term technical issue. The company was forced to stop online orders for more than six weeks, which in today's retail environment, is basically an eternity. Customer data was reportedly stolen too, and the company was also unable to process in store contactless payments- and who carries physical cards nowadays anyways. And so as a consequence, M&S reported that profits for the six-month period that followed the attack had halved, showing clearly how cyber attacks can have a very real and material impact on a company's financials.

And what made these attacks on UK retailers particularly disruptive was that they didn't just involve data like your personal details or financial information. They affected payments, logistics, and day-to-day operations. The kinds of things customers

notice immediately and the kinds of things retailers rely on to keep shelf stocked and tills working. And these weren't isolated cases.

If you cross the Atlantic, the world's largest meat processing company, JBS, was targeted by a ransomware attack that forced it to shut down operations in many countries. The company had to pay \$11 million to regain control of its systems and protect customer data, which raised concerns not just about corporate losses, but also about the resilience of the food supply itself. And more recently, we've also had Ahold Delhaize, one of the world's largest grocery groups based in the Netherlands, that was hit by a cyber attack that compromised the personal data of more than two million people. Taken together, these incidents point to something bigger than a series of one-off cyber events.

They reveal a sector that has become deeply digital and highly interconnected, and in some cases, more fragile than it appears. To tell us why food retailers are particularly at risk, I talked to my colleague Cole Martin out of our London office. Here's Cole.

Speaker 2: So, there are a couple of things to unpack here. Firstly, if you think about the food retail industry, you've got a low margin business model in a highly competitive landscape involving companies that often have up to hundreds of thousands or even literally millions of employees.

Second, how are retailers trying to involve in this environment? Well, among other things, they are leaning into digitization and AI. They're doing this to both streamline their operations to cut costs and to try to drive foot traffic through enhanced customer experiences that ultimately drive revenue growth. And this evolution means that they're storing ever more of their own and customer data online, which may increase the risks and damage related to cyber attacks.

As I alluded to earlier, if you're a very large food retailer, you might have hundreds of thousands of employees. Now, most of those employees, especially the frontline employees, probably won't have access to, for example, personalized company email addresses, but store managers might. And that means that hundreds, if not thousands of employees, could be social engineering targets for hackers in any one company.

Not to mention that even if you have even a small amount of turnover, that means hundreds of new employees to get up to speed on the information security protocols. And furthermore, even if you thoroughly train your own employees, you could end up with a breach because of a contractor or a supplier, which is relatively common within the industry. And of course, that's what happened to Marks and Spencer.

Now, maybe you thought ahead and bought cyber insurance, which will protect you to some extent. But if you or your competitors get hacked, it stands to reason that the cost of insurance is going to go up, which could impact operating profits and ultimately free cashflow.

Speaker 1: So, it makes sense that cyber attacks are becoming a more and more common risk for the sector. The key question then becomes, how do we tell which companies

are actually prepared to deal with that risk? Using our ESG ratings data, one way to look at this is through how companies manage privacy and data security risks. We won't get into the weeds of the model now, but at a high level, this risk matters most for businesses that handle large volumes of personal data or face costly data breaches, which based on our data, is increasingly the case for food retailers.

In practice, cyber risk in food retail shows up in two main ways. One is operational disruption, so systems going down, payments failing, and so on. The other is data breaches, so where customer information is exposed and potentially leading to reputational damage or regulatory fines like under GDPR.

What really separates companies here though is preparedness. And here, our data suggests that many large food retailers still sit in the middle of the pack or behind when it comes to managing these risks. That comes down to basics like employee training, data security systems and certifications and breach response plans.

Companies tend to fall along a spectrum, so from meeting bare minimum requirements to adopting more robust practices. But on these fronts, companies like Marks & Spencers and its UK peers, Tesco and Sainsburys, don't currently follow industry-leading practices. For example, a leading practice would mean that a company ensures that all employees, full-time, part-time, and contractors receive comprehensive training on privacy and data security, but many retailers still limit this to parts of their workforce only.

And so if that gap between rising risk and lagging practices persists, it opens the door to a bigger question about how serious and potentially how systemic these cyber threats could become.

Here's Cole.

Speaker 2: So, you never want to speak something into existence, but one darker thought I had is this. At what point do these types of cyber attacks become a national security issue? Up 'til now, many of the hacks like the ones mentioned earlier were done for criminal purposes or by agents of chaos, but there's been a lot of chatter in the media, and for example, in foreign policy circles about the rise of non-linear or asymmetric conflicts.

And so given how concentrated the food retail industry is in many countries and how little slack there is in the food production system with just-in-time inventory, management, systems, etcetera, you wonder if these types of attacks are something that could be exploited by highly sophisticated state level or state-adjacent actors. Like for example, suppose you're a country or region that has a highly concentrated meat production industry and a consolidated food retail industry, maybe three or four companies in each industry per country or region.

If you knocked one of these companies offline for several months through a very sophisticated cyber attack, that may well have an impact on food price inflation. And given how sensitive consumers are to this, this may well affect electoral or broader political

outcomes. Ultimately, food retailers could be increasingly vulnerable to the type of cyber attacks that we know at the very least could have a significant impact on a company's profits and stock.

Lots of things affect share prices, as we know, but I think it's very notable that M&S's share price was doing really well in the two years leading up to their cyber attack, and it's kind of been floundering ever since. So, if I'm an investor in companies in this industry, personally, I'd be interested in figuring out how companies are going to try to manage these risks through better practices, and also manage the trade-off between investing in cybersecurity solutions without damaging their operating margins in the context of increasing digitization and AI adoption.

Speaker 1: And that is it for the week. A massive thanks to Cole for his take on the news with a sustainability twist, and thanks to you as well for listening and sticking around. If you liked this episode, don't forget to subscribe and maybe even share it with a friend or colleague. That's all from me. Thanks again and catch you next week.

Speaker 3: The Sustainability Now Podcast is provided by MSCI Solutions, LLC, a subsidiary of MSCI, Inc. Except with respect to any applicable products or services from MSCI solutions, neither MSCI nor any of its product or services recommends, endorses, approves, who otherwise expresses any opinion regarding any issuer, securities, financial products, or instruments or trading strategies. And MSCI's products or services are not intended to constitute investment advice or recommendation to make or refrain from making any kind of investment decision and may not be relied on as such. The analysis discussed should not be taken as an indication or guarantee of any future performance, forecast, or prediction.

The information contained in this recording is not for reproduction in whole or in part without prior written permission from MSCI solutions. Issue is mentioned or included in any MSCI solutions material may include clients of MSCI or suppliers to MSCI and may also purchase research or other products or services from MSCI Solutions.

MSCI Solutions materials, including materials utilized in any MSCI sustainability and climate indexes or other products have not been submitted to nor received approval from the United States Securities and Exchange Commission or any other regulatory body. The information provided here is as is, and the user of the information assumes the entire risk of any use it may make or permit to be made of the information. Thank you.

## About MSCI

MSCI is a leading provider of critical decision support tools and services for the global investment community. With over 50 years of expertise in research, data and technology, we power better investment decisions by enabling clients to understand and analyze key drivers of risk and return and confidently build more effective portfolios. We create industry-leading research-enhanced solutions that clients use to gain insight into and improve transparency across the investment process. To learn more, please visit [www.msci.com](http://www.msci.com).

---

This document and all of the information contained in it, including without limitation all text, data, graphs, charts (collectively, the "Information") is the property of MSCI Inc. or its subsidiaries (collectively, "MSCI"), or MSCI's licensors, direct or indirect suppliers or any third party involved in making or compiling any Information (collectively, with MSCI, the "Information Providers") and is provided for informational purposes only. The Information may not be modified, reverse-engineered, reproduced or redisseminated in whole or in part without prior written permission from MSCI. All rights in the Information are reserved by MSCI and/or its Information Providers.

The Information may not be used to create derivative works or to verify or correct other data or information. For example (but without limitation), the Information may not be used to create indexes, databases, risk models, analytics, software, or in connection with the issuing, offering, sponsoring, managing or marketing of any securities, portfolios, financial products or other investment vehicles utilizing or based on, linked to, tracking or otherwise derived from the Information or any other MSCI data, information, products or services.

The user of the Information assumes the entire risk of any use it may make or permit to be made of the Information. NONE OF THE INFORMATION PROVIDERS MAKES ANY EXPRESS OR IMPLIED WARRANTIES OR REPRESENTATIONS WITH RESPECT TO THE INFORMATION (OR THE RESULTS TO BE OBTAINED BY THE USE THEREOF), AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EACH INFORMATION PROVIDER EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES (INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF ORIGINALITY, ACCURACY, TIMELINESS, NON-INFRINGEMENT, COMPLETENESS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE) WITH RESPECT TO ANY OF THE INFORMATION.

Without limiting any of the foregoing and to the maximum extent permitted by applicable law, in no event shall any Information Provider have any liability regarding any of the Information for any direct, indirect, special, punitive, consequential (including lost profits) or any other damages even if notified of the possibility of such damages. The foregoing shall not exclude or limit any liability that may not by applicable law be excluded or limited, including without limitation (as applicable), any liability for death or personal injury to the extent that such injury results from the negligence or willful default of itself, its servants, agents or sub-contractors.

Information containing any historical information, data or analysis should not be taken as an indication or guarantee of any future performance, analysis, forecast or prediction. Past performance does not guarantee future results.

The Information should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. All Information is impersonal and not tailored to the needs of any person, entity or group of persons.

None of the Information constitutes an offer to sell (or a solicitation of an offer to buy), any security, financial product or other investment vehicle or any trading strategy.

It is not possible to invest directly in an index. Exposure to an asset class or trading strategy or other category represented by an index is only available through third party investable instruments (if any) based on that index. MSCI does not issue, sponsor, endorse, market, offer, review or otherwise express any opinion regarding any fund, ETF, derivative or other security, investment, financial product or trading strategy that is based on, linked to or seeks to provide an investment return related to the performance of any MSCI index (collectively, "Index Linked Investments"). MSCI makes no assurance that any Index Linked Investments will accurately track index performance or provide positive investment returns. MSCI Inc. is not an investment adviser or fiduciary and MSCI makes no representation regarding the advisability of investing in any Index Linked Investments.

Index returns do not represent the results of actual trading of investible assets/securities. MSCI maintains and calculates indexes, but does not manage actual assets. The calculation of indexes and index returns may deviate from the stated methodology. Index returns do not reflect payment of any sales charges or fees an investor may pay to purchase the securities underlying the index or Index Linked Investments. The imposition of these fees and charges would cause the performance of an Index Linked Investment to be different than the MSCI index performance.

The Information may contain back tested data. Back-tested performance is not actual performance, but is hypothetical. There are frequently material differences between back tested performance results and actual results subsequently achieved by any investment strategy.

Constituents of MSCI equity indexes are listed companies, which are included in or excluded from the indexes according to the application of the relevant index methodologies. Accordingly, constituents in MSCI equity indexes may include MSCI Inc., clients of MSCI or suppliers to MSCI. Inclusion of a security within an MSCI index is not a recommendation by MSCI to buy, sell, or hold such security, nor is it considered to be investment advice.

Data and information produced by various affiliates of MSCI Inc., including MSCI ESG Research LLC and Barra LLC, may be used in calculating certain MSCI indexes. More information can be found in the relevant index methodologies on [www.msci.com](http://www.msci.com).

MSCI receives compensation in connection with licensing its indexes to third parties. MSCI Inc.'s revenue includes fees based on assets in Index Linked Investments. Information can be found in MSCI Inc.'s company filings on the Investor Relations section of [msci.com](http://msci.com).

MSCI ESG Research LLC is a Registered Investment Adviser under the Investment Advisers Act of 1940 and a subsidiary of MSCI Inc. Neither MSCI nor any of its products or services recommends, endorses, approves or otherwise expresses any opinion regarding any issuer, securities, financial products or instruments or trading strategies and MSCI's products or services are not a recommendation to make (or refrain from making) any kind of investment decision and may not be relied on as such, provided that applicable products or services from MSCI ESG Research may constitute investment advice. MSCI ESG Research materials, including materials utilized in any MSCI ESG Indexes or other products, have not been submitted to, nor received approval from, the United States Securities and Exchange Commission or any other regulatory body. MSCI ESG and climate ratings, research and data are produced by MSCI ESG Research LLC, a subsidiary of MSCI Inc. MSCI ESG Indexes, Analytics and Real Estate are products of MSCI Inc. that utilize information from MSCI ESG Research LLC. MSCI Indexes are administered by MSCI Limited (UK).

Please note that the issuers mentioned in MSCI ESG Research materials sometimes have commercial relationships with MSCI ESG Research and/or MSCI Inc. (collectively, "MSCI") and that these relationships create potential conflicts of interest. In some cases, the issuers or their affiliates purchase research or other products or services from one or more MSCI affiliates. In other cases, MSCI ESG Research rates financial products such as mutual funds or ETFs that are managed by MSCI's clients or their affiliates, or are based on MSCI Inc. Indexes. In addition, constituents in MSCI Inc. equity indexes include companies that subscribe to MSCI products or services. In some cases, MSCI clients pay fees based in whole or part on the assets they manage. MSCI ESG Research has taken a number of steps to mitigate potential conflicts of interest and safeguard the integrity and independence of its research and ratings. More information about these conflict mitigation measures is available in our Form ADV, available at <https://adviserinfo.sec.gov/firm/summary/169222>.

Any use of or access to products, services or information of MSCI requires a license from MSCI. MSCI, Barra, RiskMetrics, IPD and other MSCI brands and product names are the trademarks, service marks, or registered trademarks of MSCI or its subsidiaries in the United States and other jurisdictions. The Global Industry Classification Standard (GICS) was developed by and is the exclusive property of MSCI and S&P Global Market Intelligence. "Global Industry Classification Standard (GICS)" is a service mark of MSCI and S&P Global Market Intelligence.

MIFID2/MIFIR notice: MSCI ESG Research LLC does not distribute or act as an intermediary for financial instruments or structured deposits, nor does it deal on its own account, provide execution services for others or manage client accounts. No MSCI ESG Research product or service supports, promotes or is intended to support or promote any such activity. MSCI ESG Research is an independent provider of ESG data.

Privacy notice: For information about how MSCI collects and uses personal data, please refer to our Privacy Notice at <https://www.msci.com/privacy-pledge>.