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.

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**.

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.

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.