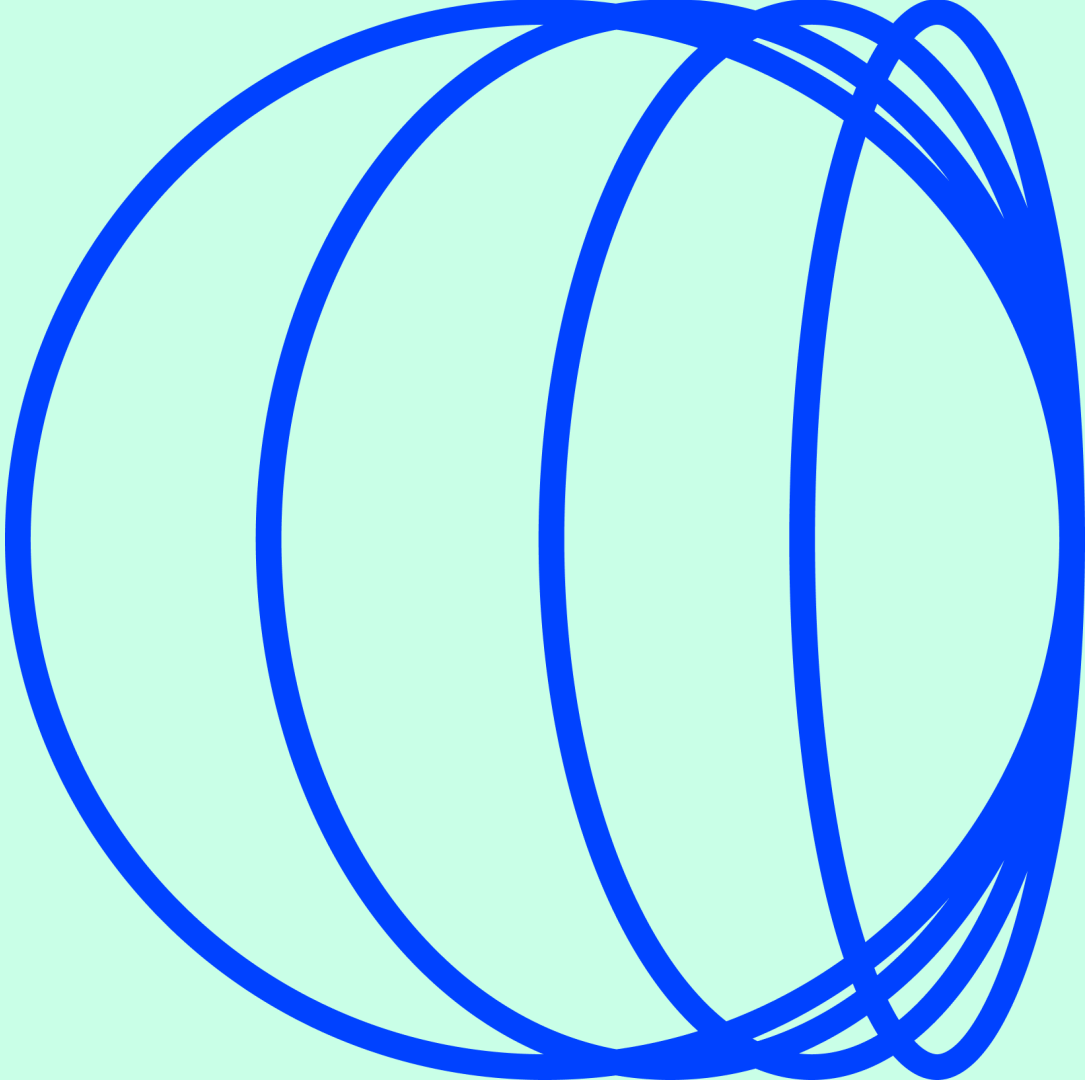
vuelio

Retail cyberattacks & the UK press reaction



Introduction & methodology

Retailers depend on trust and confidence – but a series of cyberattacks have seen brands battling to preserve their relationship with consumers.

With a growing number of organisations becoming ensnared in their own cyber crisis this year, comms teams must plan for the potential of a data breach dilemma, and the press coverage that comes with it.

In this report, we examine media coverage of UK cyberattacks, the role of crisis comms, and what PR teams in the retail space, and beyond, can learn.

Using **Vuelio Media Monitoring** and the **Journalist Enquiry Service** this report unpacks:

- How the UK press has reported on cyberattacks and data breaches impacting organisations and brands.
- What journalists and broadcasters covering this growing issue are requesting from PR & comms professionals for their reporting and write ups.
- Why both proactive and reactive PR strategies are vital for organisations at risk of cyberthreats.

Approach

Data Collection Period: 20 May 2024 – 19 May 2025

- Online News
- X
- Journalist Enquiry Service

Channels: Markets/Languages: UK data collection. Analysis in English language.

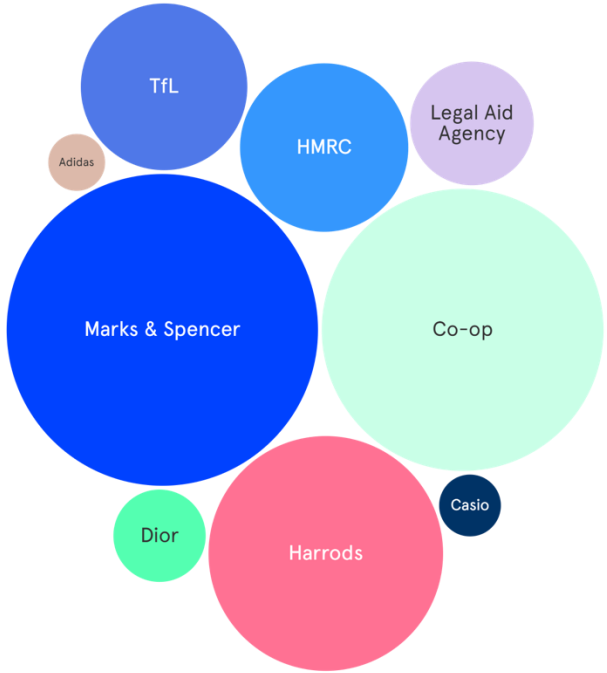
vuelio

Coverage of brands with cyber crises over the last year

Data breaches are a danger for every organisation with an online presence in the hyper-connected landscape consumers and stakeholders are now accustomed to when shopping, filing taxes, and asking for aid. But the last year has been a landmark time for testing company crisis comms strategies to their limit.

A growing number of household-name businesses, global brands, and government authorities have been the target of cyberattacks, with the UK press quick to cover the stories. The marks of these malicious attacks have varied – Adidas' help desk data delved into; the House of Dior's customer database ransacked; and HMRC hit with a reported £47 million phishing attack. But unsurprisingly, most of interest to the UK media have been tales of the travails closest to home – in the offices of our biggest retail stores.

Tracking UK media coverage of cyberattacks over the last year highlights the keen interest taken in UK high street-located brands above and beyond other organisations – even global brands. Their respective comms teams have had to be ready to answer the press, and the public's, questions as the stories spread.



Size of UK online news coverage related to specific brands impacted by cyberattacks, from 20 May 2024 to 19 May 2025. Source: Vuelio Media Monitoring.

vuelio

Press coverage of cyberattacks and data breaches

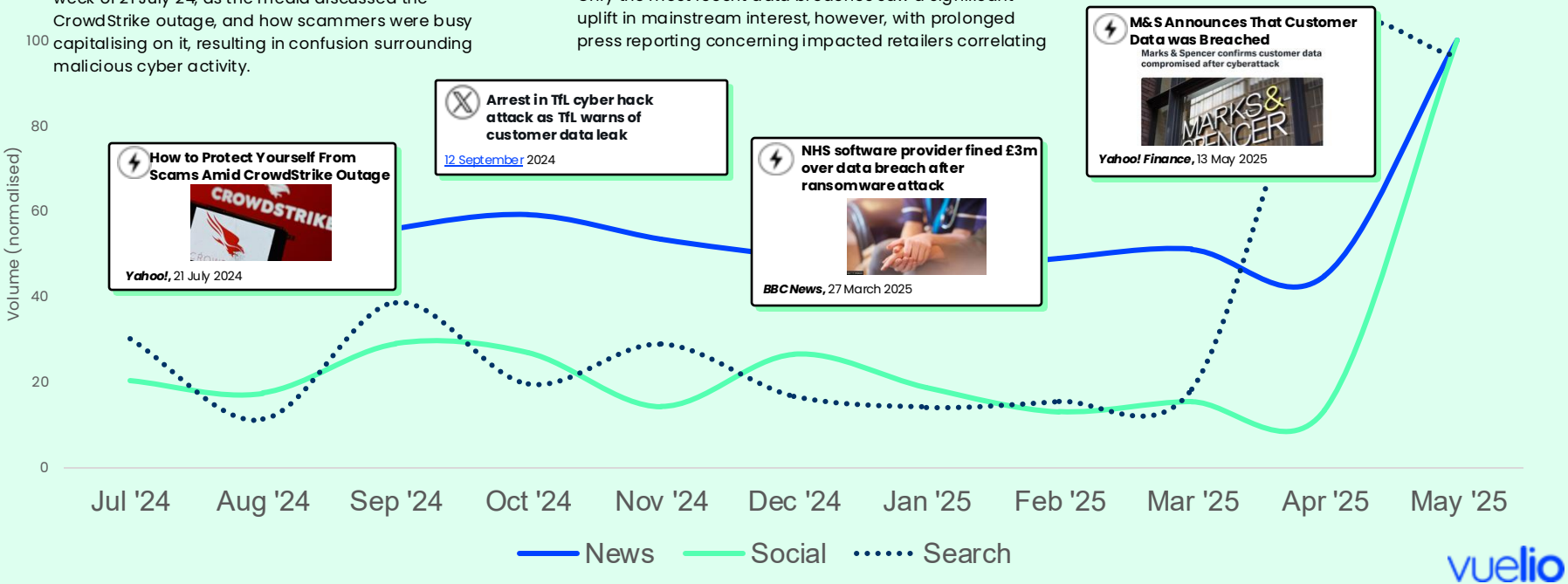
Coverage of UK cybersecurity attacks on social and in traditional media followed a similar pattern, characterised by sustained and increasing media interest.

Volumes of online coverage started to grow during the week of 21 July 24, as the media discussed the CrowdStrike outage, and how scammers were busy capitalising on it, resulting in confusion surrounding malicious cyber activity.

The second most notable peak in online coverage occurred the week of 15 September, when TfL announced that customer data had been accessed during a cyberattack. Headlines from national outlets set the tone for the conversation that played out on social media.

Only the most recent data breaches saw a significant uplift in mainstream interest, however, with prolonged press reporting concerning impacted retailers correlating with searches for information on the attacks on Google.

Official statements from the impacted retailers also caused spikes in reporting. Comms directly influenced coverage, highlighting the vital role PR plays during a crisis.



Online, Social and Google Trend data for Cybersecurity Attacks

UK media requests for reports on the cyberattacks

As the cyberattack story continues to spread across UK news platforms, journalists and broadcasters are busy sending requests for data, spokespeople, and case studies via the ResponseSource Journalist Enquiry Service. As of 27 May, 70 enquiries had already been submitted to PRs regarding the cyberattacks since 22 April, and they aren't stopping. The majority have used M&S – the first UK retail brand to fall under the crosshairs in 2025 – as a case study, posing questions to retail, financial, and tech experts on what the growing danger of cyberattacks could mean for the retail industry at large.

Those researching for reports so far come from a mix of national press and broadcast news, as well as business, retail, and trade outlets – not yet consumer. But this is no guarantee that the story won't spread to general consumer and lifestyle publications, who have wide reach among audiences that would traditionally shop with the retail brands being impacted, and those at risk in the future.

As shown in press coverage over the last month, and in media requests being sent to UK PRs: without proactive outreach from brands with official statements, journalists will seek commentary and angles elsewhere…

'The unfolding M&S incident (followed by the Co-op) has made retailers sit up and pay attention: so what are they doing to protect themselves? Taking on more IT staff? Taking cyber security services in-house?

'We have heard that at many businesses there is no leadership or ownership of cyber security as it is taken care of mainly by agencies or freelancers, with few permanent IT staff, leading to chaos. Are retailers re-thinking this approach, if so what are they doing right now to address it?

'In terms of systems and technology, are they quickly working to replace old tech? Testing systems (if so, how) and identifying weaknesses?'

Request submitted via the Journalist Enquiry Service, May 2025

'Need specific comments on M&S, Harrods, Legal Aid, and Co-op cyberattacks Information on why, what businesses can do, who was most impacted, the consequences of attacks.

'Would be good to explain why these attacks are now on the rise.'

Request submitted via the Journalist Enquiry Service, May 2025

'M&S customers continue to be affected by the cyber incident, as they still can't place orders online or in store.

- What should customers do if they need to buy something but can't place an order?
- When will M&S get its services back to normal?
- What can consumers / shoppers do to avoid being majorly impacted by incidents such as this cyber incident?'

Request submitted via the Journalist Enquiry Service, May 2025

'I am writing a piece off the back of the recent M&S and Co-op hacks to highlight tips on how to protect your financial data.

'Seeking comments on the best way to protect yourself from a hack

'Should you avoid online shopping? Is paying by cash safer than contactless?

'Are there any tools or apps that will show you if your data has been accessed/hacked?'

Request submitted via the Journalist Enquiry Service, May 2025

Source: ResponseSource Journalist Enquiry Service

vuelio

The crisis contagion

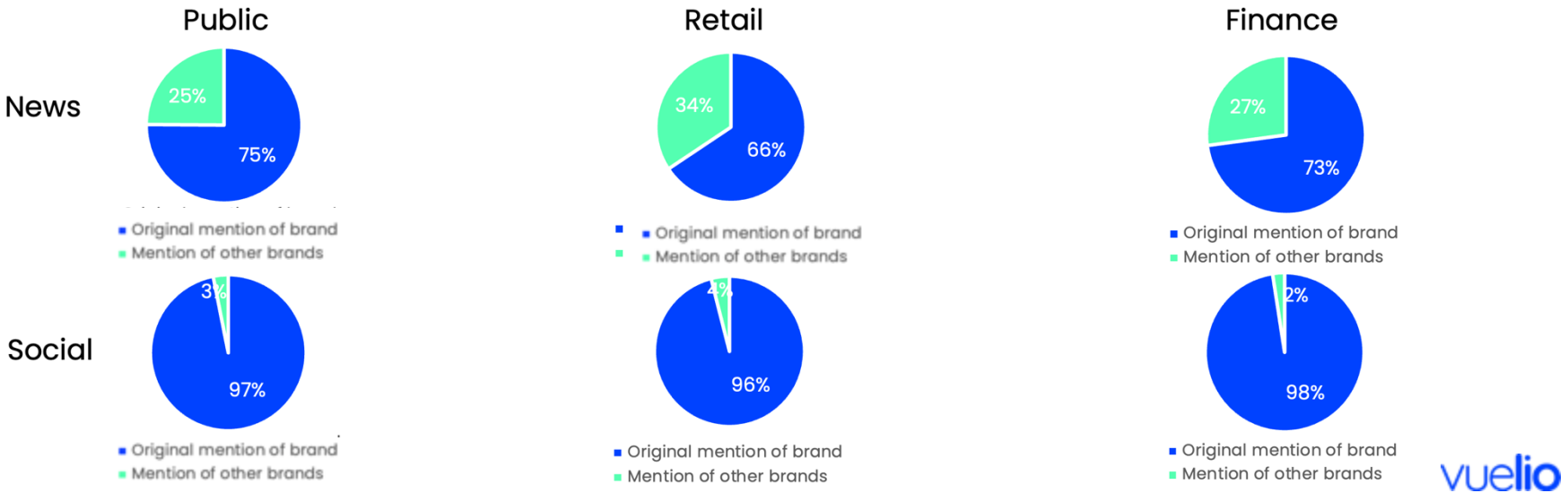
When cybersecurity hits the mainstream press, the victim of the attack is in the spotlight. However, traditional media regularly refers to how this may have an impact on other organisations. Your brand can be damaged (or boosted) by cyberattacks taking place in your sector.

Vuelio analysed key cyber security attacks in three sectors – Public Retail, and Finance – and found that contagion, the idea that an issue may have a knock-on effect in its sector, was more prolific in online coverage than in conversations on social media. Social media posts about Public Sector attacks, which affected organisations like TfL, focused on ongoing updates, rather than drawing comparisons to other organisations who have historically been affected.

The retail sector had the highest share of contagion coverage. M&S' was heavily influenced by other retailers' news of the incidents, AOL's 'Hackers target the Co-op as police probe M&S cyber attack' just one example.

The Finance sector followed the same trends, having more contagion coverage in online media, including strategies that organisations were putting in place to prevent potential customer data breaches.

We don't see much consumer media coverage; however, as the implications for consumers become clearer, we can expect this to rise – even as mainstream media interest may shift elsewhere.



Online and social media mentions of Cyber Security Attacks in the UK, Social and Traditional

The role of reactive PR

Cyberattacks are a problem that will be faced by an increasing number of organisations as we move further into a digital-first AI-enabled business world. But these 'new' problems for brands can be met with established weaponry from the PR toolbox – reactive comms.

Official statements from company CEOs are a tried and trusted tactic for big brands who need a human face when a crisis hits. Highlighting just how effective this can be as part of a reactive PR strategy are reports of specific UK cyberattacks. M&S CEO Stuart Machin's statement was greeted with a mix of positive and neutral reactions, with the brand presented as being more on the forefront of a widespread issue than being particularly culpable.

Other impacted brand CEO statements of apology have moved the spotlight to different, unrelated issues impacting consumers who wish to continue shopping with them. In comparison, Chief Exec statements that have focused on future prevention rather than apology have sparked press coverage that centres their brand as a figurehead for minimising the harm of cyberattacks, as well as how to retain customer loyalty and trust.

Cyberattacks are an issue that won't go away for retail soon – proactive and reactive comms strategies will continue to be vital.

The Guardian
2 May 2025


Co-op apologises after hackers extract 'significant' amount of customer data

The National Cyber Security Centre and the National Crime Agency are assisting with an inquiry, the group said

'Co-op apologises after hackers extract 'significant' amount of customer data'

Drapers
6 May 2025


What are retailers investing in now to bolster cyber-security?

BY NICOLA SMITH 6 MAY 2025

As Marks & Spencer continues to battle with a major ransomware attack, Drapers explores the tools and techniques retailers must invest in to fortify their cyber-security defences.

'What are retailers investing in now to bolster cyber-security?'

Financial Times
8 May 2025


Retailers face 10% hikes to premiums after cyber attacks

Recent ransomware attacks and data breaches are expected to push up rates for the sector

'UK retailers face 10% rises in premiums after cyber attacks

The London Standard
20 May 2025


NEWS | TECH

All the major cyber attacks in the UK this year: Are they on the rise?

British companies have toppled like dominoes at the hands of cyber criminals. What happened and are these attacks the new norm?

'All the major cyber attacks in the UK this year: Are they on the rise?'

BBC News
24 May 2025

'Inside the high street cyber attacks'

Online and social references to the respective CEO's apologies and strategic comms. Source: Vuelio Media Monitoring.

vuelio

Differing coverage themes for impacted brands

How an organisation responds to a crisis can make or break their reputation. We took three impacted brands and examined their strategies when it comes to communicating with the press...

Harrods

This brand had the lowest share of coverage about the **Nature of Attack**, being able to restrict the hackers' access before any customer data was reached. However, the organisation had the largest share of coverage about **Future Prevention**. The attack prompted cybersecurity professionals like Devon Kerr to discuss the need for retailers to invest in more secure systems .

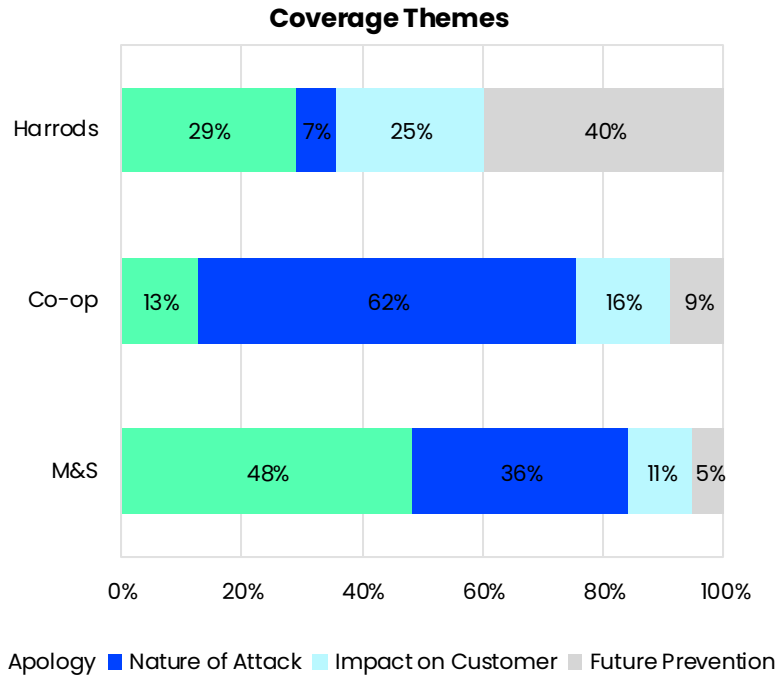
Co-op

Nature of Attack was this brand's most prominent theme (62%). The organisation was the first to announce that customer data had been breached. Coverage was prominent across both social and traditional media, and perhaps more widely discussed due to the organisation being the first to put its head above the parapet regarding a breach, or because of heightened media attention due to announcing the attack the day before. **Impact on Customer** was the second most prominent theme as the media discussed delivery delays and 'empty shelves'. Coverage with this theme peaked on 6 May as Co-op released an operational update.

M&S

The **Apology** theme had the largest share for this brand, which was one of the first retailers to announce it had been affected by the cyberattacks. However, being slow to announce how the cyber attack had impacted its customers, this retailer was the target for a significant amount of press attention, not all of it positive.

Organisations wishing to avoid long-term press coverage – Future Prevention comms is a wise strategy to stop extra speculation in its tracks.



Online and social media mentions of three retail brands in relation to their respective cyberattacks between 22April and 19 May. Source: Vuelio Media Monitoring.

vuelio

Vuelio's head of insights **Amy Chappell** on the value of strategic planning

'The evolving media landscape around cyber attacks in the UK underscores the critical role of strategic communication in shaping public perception in today's hyper-connected landscape.

'Our ongoing analysis of these crises highlights just how valuable it is to have the right tools and data-driven insights at hand — empowering communicators to respond quickly, transparently, and with confidence, and ultimately take control of the narrative when it matters most.'

Lessons for comms teams facing a cyber crisis

Cyberattack stories will continue to be sought out by the UK press

Media coverage of cyberattacks reached a peak in April of this year in the UK, and media requests from journalists and broadcasters show they will be quick to return to the well when further organisations are hit by a hack. Have a crisis strategy planned and ready.

Not at risk? Your competitors could be

Even organisations without their own cyberattack can be hit by crisis if contagion comes into play. Monitor your competitors, and your sector, for upcoming threats as well as opportunities to provide industry expertise and comment to the press.

Speak up, or wait until the dust settles?

Analysis of official press statements from brands impacted by cyberattacks in 2025 shows that early comment to the press can help stop a story from spinning out of a comms team's control. Slower, drawn out, communications to the press and public can result in continuing – potentially damaging - coverage. Don't leave a vacuum to be filled with speculation. Proactive comms are as important as reactive responses.

Apologies – good. Plans for prevention – better

While ownership and acknowledgement of responsibility can lead to positive press reaction, plans for future prevention do better. Transparency regarding future proofing is what will reinforce, or recover, brand loyalty.

vuelio

How Pulsar Group can help with your PR strategy & comms

Vuelio Media Monitoring: Prove the effectiveness of your PR & comms tactics and provide a base for future planning through multi-channel media coverage categorised by sentiment, Share of Voice, and bespoke tags.

Vuelio Insights: The Vuelio Insights team partners with clients to produce bespoke media analysis reports that identify risks and opportunities, and demonstrate the value of your PR.

Vuelio Political Monitoring: Vuelio gives you full visibility of everything that's happening across Government, Parliament, stakeholder organisations, and social media, delivered in a way that works for you.

Journalist Enquiry Service: Get journalist enquiries delivered straight to your inbox so you can connect and secure coverage for your organisation at top UK media outlets.

Authors:

P-J Boyd
Comms & Content Manager
pj.boyd@vuelio.com

Xena Perryman
Insights Executive
xena.perryman@vuelio.com

Amy Chappell
Head of Insights
amy.chappell@vuelio.com

PULSAR*GROUP

vuelio